Online Security and Privacy Awareness of Activists

Long-Term Design Case Study of
Technology and Social Media Use by Activists in Republika Srpska
and Development of the Application Cyberactivist

Dipl.-Ing. BORISLAV TADIĆ, Bakk.rer.soc.oec.

An der Fakultät III:

Wirtschaftswissenschaften, Wirtschaftsinformatik und Wirtschaftsrecht

der Universität Siegen

zur Erlangung des akademischen Grades

Doktor rerum politicarum (Dr. rer. pol.)

Erstgutachter: Prof. Dr. Volker Wulf

Zweitgutachter: Dr. Markus Rohde

Abstract

Bosnia-Herzegovina and its entity, Republika Srpska are among the most fragile democratic post-war environments in Europe. During the initial phase of our long-term participatory design case study, we engaged with the main activists in the region, which led to the structured view of their information and communication technology practices, benefits, needs, and the various constraints under which they act. This analysis highlighted the interest in the ICT, as well as the intense use and dependency of social media for the activists in the region, resulting in more efficient access to their target group, easier information sharing with general society and international community, and faster reaction to the "offline" activities. Simultaneously, it shed light on the limited budgets and project sustainability, low knowledge level around ICT use and maintenance of the activists, high dependency of the external stakeholders and outsourcing, and a major lack of awareness regarding privacy and security.

We concluded that the socio-political activists in RS, but also in the other regions such as Middle East and North Africa, or Southeast Asia are very exposed, often unaware, or ignorant of the risks and lack the remediation measures, esp. related to the secure, private, and anonymous network and social media use. The work on the development of privacy and security tools has not always recognized the nature of the political processes in emerging democracies and authoritarian regimes, frequent naivety about threat, nor the "occasioned" responses of activists because activism can be a "one time" endeavor, prompted by specific events. Using the combination of qualitative content analysis, field/empirical studies and abduction based on grounded theory, a four-layer, "pyramidal" threat model was derived. This model describes defamation, legal action, material loss and physical harm, and sensitizes activists to the range of threats they might be subject to in the context of security and privacy.

Due to the rising number of threats and impact of the recent incidents in this domain, we created a technical design Cyberactivist to raise security and privacy awareness within activist circles and non-profit organizations. We applied iterative, participatory design to create the prototype and offered the free web application to RS/BH activists for testing. Their feedback helped us to focus and develop the next version of the tool, which supports activists by raising awareness, challenging ignorance, lowering exposure, and enabling remediation within the privacy and security domain. Authors then again engaged with RS, but also international activists and HCI activism researchers to assess the global applicability of Cyberactivist. Based on this qualitative feedback we defined the functional and non-functional requirements for the tool improvement, and through several iterations, further addressed "usable security" and "privacy by design" to ensure its better applicability. We also elaborated why the design of the corresponding target-group trainings based on our lessons learned would complement the Cyberactivist, and further raise awareness and enable risk remediation.

Acknowledgement

I am deeply grateful to my mentors and thesis advisors Prof. Dr. Volker Wulf and Dr. Markus Rohde for the close guidance and thorough support of my research activities at the intersection between Software Engineering, Human-Computer Interaction and Computer Supported Cooperative Work over the previous years. Furthermore, I thank Dr. David Randall for his kind advice and fruitful cooperation on various papers.

Without the continuous encouragement of my parents Zoran and Stela, my brother Igor, my wife Jovana, and close friends this dissertation would not have been written. The joy from the birth of my son David in 2022, finally boosted my output and led to the completion of this endeavor. In addition, I would like to express my gratitude to Dr. Thomas Kremer and Andrei Svirida who opened space for me to conduct my research, participate in the conferences and reminded me to stay on track during the work-intense times.

I would also like to thank Konstantin Aal and other colleagues from the University of Siegen, as well as Ognjen Stefanovic who provided me with examples, coding support and feedback, during the tool development. I also sincerely thank all the participants of my study and various activists world-wide who allowed me to conduct open interviews and make observations that brought this research to the next quality level, and who have chosen to remain anonymous in this dissertation.

Author Information

At the time this dissertation was submitted, Borislav Tadić is Senior Vice President responsible for the Deutsche Telekom Technology North focusing on the high-speed network rollout and maintenance with over 150 teams spread throughout Germany. Prior to this role, he led cross-functional teams and programs in the "Data Security, Compliance & Legal", Center for Strategic Projects, Business Development & Partnering in the USA, Multi-Regional Security Management at Corporate IT of Deutsche Telekom and Detecon in Switzerland, Africa, and Asia-Pacific Region. Borislav gathered leadership experience in more than twenty-five countries on four continents and within eight industries (e.g., Siemens, United Nations, Fraunhofer, Magna, IREX).

Borislav holds a master's degree (Dipl.-Ing.) in Software development & Economy and bachelor's degree in Software Development and Knowledge Management (Bakk.rer.soc.oec.) from University of Technology in Graz, Austria. As a holder of numerous awards and certifications, he coaches many talented individuals and engages in numerous non-profit, academic and professional formats. Borislav's contributions were published in various printed and online editions and broadcasted over numerous radio and TV stations worldwide. He fluently speaks several languages, enjoys travelling (seventy-five countries visited) and sports, and in addition to Hamburg, Banja Luka, Graz, and Bonn, he lived in Zürich, Johannesburg, and San Francisco.

Declaration of Authorship

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where stated otherwise by reference or acknowledgment, the work presented is entirely my own.

Hamburg, 31.10.2022 _____

Contents

List of Figures

List of Tables

List of Annexes

Annex I: Documents Related to the Interview

1. Information form
2. Participation form
3. Questionnaire
4. Declaration of consent and data protection declaration

Annex II: Interview Partners

Annex III: Annex to Section 4.4 of the Main Document

5. Simplified Cyberactivist Tool Tree
6. Cyberactivist Tool Self-Test
7. CyberActivist Tool Major Change History
8. Cyberactivist Tool Adaptation

Annex IV: Software Components Used for CyberActivist

Annex V: Digital Archive Submitted with this Document

Frequently Used Abbreviations

BH	Bosnia-Herzegovina
CHI	Computer-Human Interaction
CSCW	Computer-Supported Cooperative Work
CSS	Cascading Style Sheet
DCS	Design Case Study
EAR	Ethnographic Action Research
EU	European Union
EUR	EU Euro
GDPR	General Data Protection Regulative
HCI	Human-Computer Interaction
HTML	Hypertext Markup Language
ICT	Information Communication Technology
IT	Information Technology
NPO	Non-profit Organization
PbD	Privacy by Design
P&SbD	Privacy and Security by Design
RS	Republika Srpska
UI	User Interface
URL	Uniform Resource Locator
USA	United States of America
USD	US Dollar

1 Introduction

1.1 Motivation

The importance of global socio-political activism is ever-growing. “Fight for the better world” takes place not only in physical space, but also increasingly in cyber space. Campaigns around “Occupy”, “Fridays for Future”, “Black lives matter”, “#MeToo”, and Covid-19 pandemic are among many activism examples that marked the last decade in both offline and online context. Use of Information Communication Technology (ICT) and especially mobile devices and social and new media, has proven to help activists to control the information flows, mobilize its users for the cause, and more efficiently and effectively plan, coordinate, and execute activities in the physical world - from the USA (Mundt et al. 2018), over Europe (Lopreite et al. 2021) and MENA (Howard et al. 2011), to Russia (Lange-Ionatamishvili 2015) and China (Yang 2018).

However, there are numerous serious security and privacy risks related to ICT and social media which can be addressed with adequate mitigating measures, and related awareness and training measures. While the activists in the “Western world” can relate to the digital space regulation (e.g., EU General Data Protection Regulation), various ICT tools and funding for their protection, activists under authoritarian regimes and in economically weak environments often face threatening conditions if the above risks materialize. Republika Srpska (RS), autonomous entity in potential European Union candidate Bosnia-Herzegovina (BH) is “somewhere in the middle”: activists in this transitioning region face some of the traits seen on the “both poles”.

For this reason, the author, and several human-computer interaction researchers, started a long-term design case study looking at the major activities and activists in the region of BH/RS. The purpose was to apply qualitative methods to identify the essential elements of ICT and social media use with specific improvement possibilities. After the initial phase, the focus was set on often neglected aspect of privacy and security. We strived to derive possible risks and mitigating actions relevant for the target group in the frame of their resources, develop a tool “Cyberactivist” for raising awareness and ensure global applicability through dialogue about the measures and the tool with other international researchers in this domain.

1.2 Structure

This thesis includes three main parts: the first one introduces the motivation, context, and the method of the study, second one the key results; and the third one a summary of the results and implications, including the outlook. Section 1 presents the motivation for and structure of this thesis. Section 2 focuses on the context of the study and activism. Section 3 outlines the methodological framework, as esp. concepts of related concepts of CHI/CSCW, grounded theory, usable security, and privacy by design, looks at the setting, research question, participants, and approach. Section 4 then presents all relevant conference and journal articles within the design, long-term case study:

- 4.1: Tadic B., Rohde M., Randall, D., & Wulf V. (2016). ICT Use by Prominent Activists in Republika Srpska. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16) in San Jose. Association for Computing Machinery, New York, NY, USA, pp. 3364–3377. DOI: https://doi.org/10.1145/2858036.2858153.
- 4.2: Tadic, B., Rohde, M., & Wulf, V. (2018). Cyberactivist: Tool for Raising Awareness on Privacy and Security of Social Media Use for Activists. In International Conference on Social Computing and Social Media. Springer, Cham, pp. 498-510
- 4.3: Tadic B., Rohde M., Randall, D., & Wulf V. (*in submission to JCSCW*). Security and Privacy Aspects of ICT and Social Media Use by Activists in (Post-) Conflictual Societies.
- 4.4: Tadic B., Rohde M., Randall, D., & Wulf V. (2022). Design Evolution of a Tool for Privacy and Security Protection for Activists online: Cyberactivist. In International Journal of Human–Computer Interaction, pp. 1-23.
- Not included in the thesis, but may well complement the context: Aal, K., Krüger, M., Rohde, M., Tadic, B., & Wulf, V. (2019). Social Media and ICT Usage in Conflicts Areas. In Information Technology for Peace and Security by Reuter, C. (Ed.). Springer Vieweg, Wiesbaden, Germany, pp. 383-401.

Section 5 then deals with the summarized findings from across the different papers and the implications for activists, researchers, and business. This thesis offers insights that support researchers, designers, and developers, as well as the global community of socio-political activists – both in terms of the theory and information about the dynamics of the security and privacy within the ICT and social media use, as well as practically providing the tool designed to raise awareness of this specific target group. Section 6 highlights the contribution of the thesis to the field of social informatics, provides an outlook and concludes the thesis. The annexes hold further information about the sources, software code and related files.

1.3 Political Context: Activism in Republika Srpska

The Southeast European country Bosnia-Herzegovina (BH) is a very fragile, complex parliamentary democracy in Europe. Ethnic conflicts in the 1990s in the former Yugoslavia, now often referred to as the "western Balkans", have triggered major changes in society. BH was affected especially hard by the circumstances, parallel to having the most total war casualties. Although Dayton Peace Accord supported by the international community brought peace and the new constitution guaranteeing human rights (Sloan 1996), the country is still "plagued" by the slow post-war reconciliation process, high-level of unemployment, corruption and emigration, low levels of the social cohesion, and lack of political alignment on the future direction (EUReportBH 2021). The country has a potential candidate status since February 15th, 2016 (Europa.ba 2021). Although 76% of the BH population supports the EU ascension, there are groups that oppose it for distinct reasons (Dnevnik.ba 2021).

The country consists of two autonomous entities and one jointly managed district:

- Republika Srpska, RS, population of 1,228 million (Eacea 2021), roughly 25.000km^2, 49% of BH
- Federation BH, FBH, population of 2,219 million (Eacea 2021), roughly 26.000km^2, 51% of BH, consisting of 10 cantons
- Brcko District, population of 0,083 million (Eacea 2021), roughly 500km^2.

Both entities display similar traits, such as the complexity of the media space and the increase in the frequency and impact of the activists and protests, both offline and online. This dissertation focuses on RS, due to the simpler nature of the organization and the fact that the author was born and lived in the city Banja Luka prior to relocating to the EU in 2004.

1: Bosnia-Herzegovina in Europe (Wikimedia 2022)

2: Republika Srpska and District Brčko (Wikimedia 2022)

In this fast-changing, unstable environment, political activism takes on a particular flavor and is therefore important for the long-term case study. This dissertation presents results of a multi-year, qualitative, exploratory, and participative research dealing with activism. More details about the region, country, entity, ICT, and political environment can be found in Section 4. The term "Serbo-Croatian language" used in this dissertation describes the similar, but often disputed, languages and/or dialects used in RS before the war (e.g., Serbian, Croatian), during and after the war (e.g., Bosnian, Bosniak, Montenegrin).

Excluding classical offline and online political position-opposition and pre-election rallies, primary motives for activism in the western Balkans are primarily found in fight against corruption, then "injustice", division of society, but lately also on environmental topics, e.g., destruction of parks in Albania (Likmeta 2012) and mining areas such as controversial Rio Tinto deal in Serbia (Reuters 2022).

RS/BH faced several major protests in the last decade, most notably "Save the Park" of 2016 and "Justice for David" of 2018, with dozens of thousands of participants online and offline over several months. Federation of BH (FBH) faced "Babylution" anti-government protests of June 2013 and February 2014 within this scale when newborns could not obtain unique government identification due to the lack of political consensus, which have not been significantly visible in the RS for numerous reasons. Mujkic (2014) described them as protests "against social injustice and the system that produces laws and political structures that maintain their hegemonic privileges and hierarchy" (p. 217). Also, the protest who got social media attention and served as an inspiration for "Justice for David" were smaller "Justice for Dzenan" protests of 2016.

Extensive combination of ICT, social media, and offline activities, as well as the phases reminded of Sandoval-Almazan and Ramon (2014) model, similar to what we have seen in Tunisia, Israel, Iran, Egypt, and Syria (details of the comparison are in the Section 4.3/4). Growth of the social media users in case of "Justice for David", esp. in the relative context to the population in the RS, is comparable to the bigger movements, such as BlackLivesMatter (BLM) or Fridays for Future (F4F). Inside of couple of hours, BLM mobilized 10.000 people for protests through Facebook group (Mundt et al. 2018) and F4F reached tens of thousands of tags on Instagram (Aal et al. 2021).

1.4 Social and New Media Context

At the time of the writing of this dissertation leading social media and messaging platforms are WhatsApp, Instagram, and Facebook (Meta), Youtube (Alphabet), Skype and LinkedIn (Microsoft), iMessage (Apple), TikTok and WeChat (Tencent). In total they have approximately 4,5 billion users (Wearesocial 2021). Most social media platforms share logic of the hashtags to mark the popular topics, user accounts and groups, approval or like, followers or friends, publishing, commenting, and sharing of the textual and audio-visual content. They are available on both desktop and mobile devices, and often offer encryption possibility, possibility to remove content or report inadequate behavior or content, to both the users and the authorities, if the legal prerequisites are met. Some platforms actively censor the content through own editors, esp. that what is considered “fake news”, and some are forced to censor content, or are completely blocked by some states, such as case of Facebook, Instagram, and Twitter in Russia, seeing them as a threat (Milmo 2022).

Regarding the number of Internet, mobile and social media users in BH, the situation in January 2021 is as follows (Datareportal 2021):

- 2,32 million Internet users - equivalent to 71% of the total population
- 3,73 million mobile connections - equivalent to 113,9% of the total population
- 1,80 million social media users - equivalent to 55,0% of the total population.

There are no current detailed data for the RS, as one entity of BH. However, for several reasons, such as similar development, legal framework, distribution of urban and rural populations, demographics, the reader can assume proportional and similar conditions.

Understanding of the motivation, political and ICT context is particularly important for the understanding of the selection and application of the methodological frameworks described in the next section.

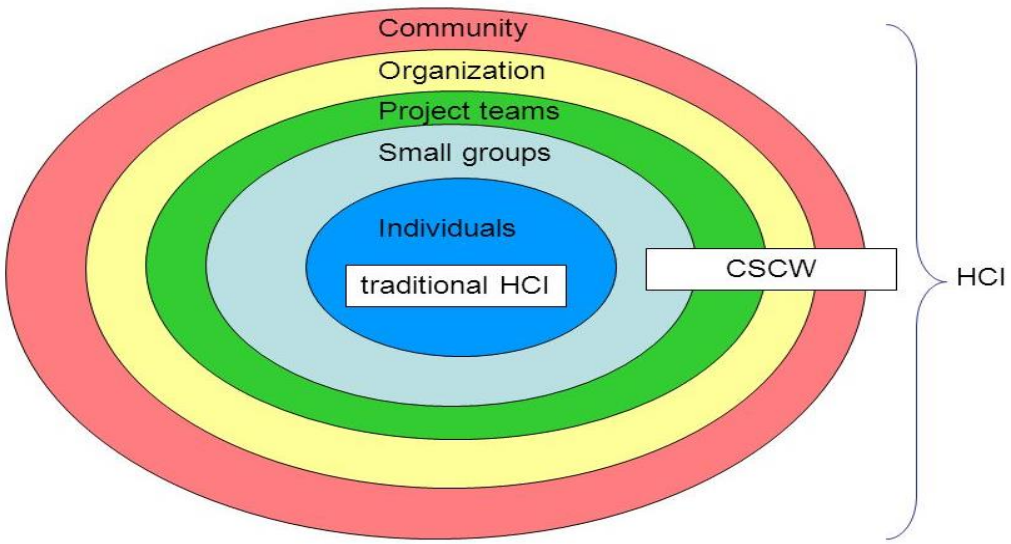
2 Method

Several research areas and approaches defined our method. For this reason, in this section we are generally introducing Human Computer Interaction and Computer Supported Collaborative Work, then Ethnographic Action Research and Design Case Studies, esp. Semi-structured and narrative interviews, as well as the Usable Security and Privacy and Security and Privacy by Design. HCI and CSCW will help to allocate and frame the relation to technology use of the socio-political activists. EAR and DCS enabled the interaction, observation, and thorough analysis, but also the experimentation and understanding of the ethnic and cultural specifics. Usable Security and PbD pointed out a research gap in this specific constellation (fragile societies, ICT, social media, interaction, impact, vulnerability) and helped focus our research contribution, as well as design the tool.

All these areas led to formulation of the objectives of the long-term design case study of technology use by activists in RS, resulting in the development of the application Cyberactivist and improvement of security and privacy awareness of the activists.

2.1 Human Computer Interaction and Computer Supported Collaborative Work

This dissertation belongs to the research domains of Human Computer Interaction and Computer Supported Collaborative Work – it references the methods and state-of-the-art from these domains and produces a unique contribution to these domains. In the case of both domains, "the computer" is general purpose term independent of the hardware, software, or system type (e.g., personal computer, smartphone app, virtualized platform).



3: HCI and CSCW in Relation (Bryan 2006)

Human-computer interaction (HCI or CHI) is “the study of the ways people interact with and through computers” (Sharples 1996). HCI grew out of work on human factors or ergonomics “with the intellectual aim of analyzing tasks that people perform with computers, and the practical concerns of designing more usable and reliable computer systems”. It also covers “the cognitive, social and organizational aspects of computer use” and describes “techniques to model people’s interactions with computers, guidelines for software design, methods to compare the usability of computer systems, and ways to study the effect of introducing new technology into organizations” (Sharples 1996, p. 293).

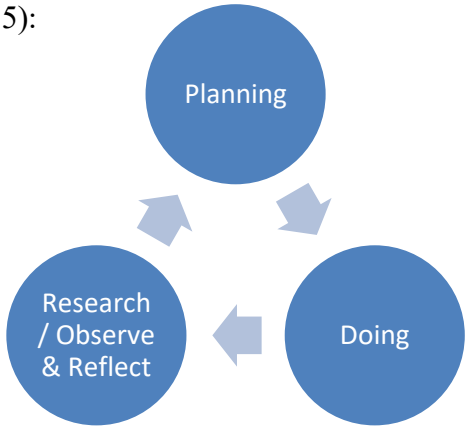
Computer Supported Collaborative Work (CSCW) combines “the understanding of the way people work in groups with the enabling technologies of computer networking, and associated hardware, software, services and techniques” (Wilson 1991). This interdisciplinary domain combines approaches of (distributed) ICT systems with information science and socio-organizational theory. Regarding our research agenda CSCW offers numerous concepts and instruments that enable complex, creative, and knowledge-intense communication, and cooperation practices within groups (Borghoff 2000).

The application of the relevant parts of these research domains and their specific methods we applied are described in detail in the following sections.

2.2 Ethnographic Action Research and Design Case Studies

Two known approaches within CHI and CSCW are ethnographic action research (EAR) and design case studies (DCS). Tacchi et al. (2003) described EAR as combination of ethnography, “traditionally been used to understand different cultures” to “guide the research process” and action research, “used to bring about new activities through new understandings of situations”, to “link the research back to the project’s plans and activities” (p.1). It is applied for the research and development of ICT projects, answering four questions throughout project lifecycle (Tacchi et al. 2003, p.5):

- What are we trying to do?
- How are we trying to do it?
- How well are we doing?
- How can we do it differently/better



4: Ethnographic Action Research

EAR follows the iterative approach, as depicted on the Fig. 4. Initial, so-called baseline research is conducted before the project starts, followed by planning and then implementation. After implementation, monitoring and evaluation research is conducted to assess how the project has developed and what are the reactions and impact on the users.

In this way, integration of the research into the continuous cycle of project planning and acting is achieved. Tacchi et al. (2003) also call it "flexible, responsive and diverse" and relate the following methods to its core:

- Observation and participant observation
- Field notes
- In-depth interviews
- Group interviews
- Diaries and other self-documentation
- ICT/Media content analysis
- Questionnaire-based sample surveys
- Public information and documentary material
- Feedback mechanisms.

Wulf et al. (2011) arguments for "dynamic relationship between ICT design and the appropriating social system", stating that as "the appropriation of ICT artifacts has a transformative effect of the given practice, at least on the micro-level, ICT artifacts should react to changing conditions of a social system" (p. 506). They also aim at "design innovative ICT artifacts whose appropriation challenges and transforms existing social practices" and suggests "case studies as a methodological framework" (p. 506).

Design case studies ideally consist of three phases (Wulf et al. 2011). In the first phase "micro-level descriptions of the social practices before any intervention takes place" are documented, esp. "existing tools, media and their usage". In the second phase, the "innovative ICT artifact from a product as well as from a process perspective" is described, along with "specific design process, the involved stakeholders, the applied design methods, and the emerging design concepts" with the focus on "how changes in social practices have been anticipated and how these considerations have influenced the design". In the third phase, "the introduction, appropriation, and potential re-design of the ICT artifact in its respective domain of practice" is documented to enable the analysis of the "transformative impact of certain functions and design options realized within the ICT artifact" (p. 506).

2.3 Semi-Structured and Narrative Interviews

Interaction, interview, and feedback are the critical elements within both EAR and DCS. In this context, the author orientated himself on qualitative research elements, such as semi-structured narrative interview.

An interview is “inter-change of views” between two actors “conversing about the topic of mutual interest” (Kvale and Brinkmann 2009). The narrative interview is one of the most prominent methods of qualitative social research. Difference to the classical quantitative interview is that the research hypothesis does not need to be checked in the interview, the research question is still open before the interview and that the hypothesis is generated from the interpretation of the interview after it has been completed (Küsters 2009).

It consists of the five phases, according to Lamnek and Krell (2005, p. 326ff):

1. Explanation phase, where the interviewees are instructed that they should speak freely and the interviewer will listen without interruption – and, if needed, their talk will be anonymized
2. Introduction: Interviewer explains which aspect is most relevant and sets one or more stimulus questions
3. Talk phase: Interviewees talk as long as they do not stop by themselves
4. Additional questions: If something is left open around the stimulus questions or if additional interesting aspects appear during the interview the interviewer can ask them
5. Summary: interviewees can talk about their experiences with the interviewer.

The fourth phase very much resonates with semi-structured interview. Semi-structured interview is “a verbal interchange where one person, the interviewer, attempts to elicit information from another person by asking questions”, and although there are predetermined questions, “participants explore issues that are important” in conversational matter (Longhurst 2003, p.143). Narrative interviews can also be done together with semi structured or structured interviews and observations (Anderson and Kirkpatrick 2016), and the author pursued this path.

2.4 Usable Security and Privacy and Security and Privacy by Design

Gerfinkel and Lipford (2014) assert that only if the researchers and designers are "simultaneously addressing both usability and security concerns will we be able to build systems that are truly secure". The reason for that is a "wide consensus that systems that are not usable will inevitably suffer security failures when they are deployed into the real world", e.g., users disclose or share passwords to ease their system access (Adams & Sasse 1999). Berkley (2021) claims that many of the privacy and security problems are "the result of a failure of system designers to consider their intended users" and describes usable security and privacy as interdisciplinary "research on human behavior to understand how people make decisions about their privacy and security, how they interact with privacy and security mechanisms, and ultimately how to design computer systems that result in privacy and security outcomes". Methods in this context include quantitative methods, such as mass surveys, measurement studies, and controlled experiments, and qualitative methods, such as interviews and ethnography.

Privacy by design is the approach to "identify and examine possible data protection problems when designing new technology and to incorporate privacy protection into the overall design, instead of having to come up with laborious and time-consuming 'patches' later on" (Schaar 2010). We can extend similar definition to security (cmp. Geismann et al. 2018).

Cavoukian (2010) defines seven foundational principles of Privacy and Security by Design, that "apply to specific technologies, business operations, physical architectures and networked infrastructure, and even to entire information ecosystems and governance models":

- Proactive not Reactive; Preventative not Remedial
- Privacy as the default
- Privacy Embedded into Design
- Full functionality – Positive-Sum, not Zero-Sum
- End-to-End Security – Lifecycle Protection
- Visibility and Transparency
- Respect for User Privacy.

Our technical design and the tool apply both PbD and Usable Security principles.

3 Long-term Case Study with RS activists

The previous subsections introduced various general concepts, and in this section, we are elaborating how we adapted and applied them to RS, our political and social media context.

In order to investigate numerous implications of the activist ICT use in a fragile democracy and derive recommendations and improvements, authors applied a palette of various methods within different fields. Table I provides an overview of the research phases with the most important results and Sections 3.1-3.4. deal with each individual phase.

3.1 Phase One

In the first phase the primary research question was – what the characteristics of the ICT use of activists in fragile, transitional democracy are. Between 2013 and 2015, the authors focused on the analysis of the local conditions, needs and communication practices of RS political activists using a mix of observational and conversational techniques.

Our first objective was the identification of the main activities in the RS where ICT and social media were intensively used in recent years. We collected data from RS-related sources in the online space and social media (e.g., popular websites, groups/pages on Facebook, "tweets" on Twitter, videos with comments on Youtube) and prominent traditional media (such as public broadcasting services, magazines, and newspaper). Then we "followed" these sources which generated most traffic over months and years (e.g., regularly reading news feeds and applying the snowball method to gain new sources). "Following" is the activation of a specific feature on social media to get regular updates on something, but also accessing a web page from an anonymous account and remaining "silent observers". Often via anonymized accounts we also read the posts and event announcements by activists, supporters, opponents and trolls and the visible reaction to those activities (e.g., comments, likes, who shared what and with whom in which context). We also sent "follow" requests to the persons/accounts on social media without interaction with them. After the initial analysis informed us about the developments, we were able to draw an initial picture of the events they were involved during and prior to that timeframe, the activist landscape and how they use(d) ICT in their engagement – all which we would refine in the later phases. It is important that some activities started prior to our research, while others continued after this phase, in one of the other forms. This also not only enabled the inclusion of precise questions into our dialogue with activists, both raising the quality of the interview and helping to understand the answers, but also provided the ideas for our later technical design.

I: Phases of Case Study on ICT Use of RS Activists

Phase *(some phases overleap)*	I: Research and interaction with RS activists and their ICT use	II: Address security and privacy of RS activists, implement prototype and first observe and reflect	III: Second observe and reflect - to optimize model and the tool	IV: Third observe and reflect - improve the tool to be more attractive for global activists
Time	2013-2015	2015-2017	2017-2018	2018-2022
Location	Online (e.g., Skype), Germany & RS	Online, RS	Online (e.g., Skype, Viber, WhatsApp), Germany & RS	Online, Germany
Participants	RS activists (6)	RS activists (7)	RS and international activists (3), CHI researchers (9)	RS and international activists (3), CHI researchers (9)
Method	State-of-the-art research, ICT traditional media content analysis, participant observation, information gathering, documentary material, in-depth, narrative, semi-structured interviews, Design Case Study	In-depth, narrative, semi-structured interviews, Field notes, Feedback mechanism, (iterative) Requirement definition, Software development, Usable Security, P&SbD	State-of-the-art research, In-depth, narrative, semi-structured interviews, group interviews, field notes, field notes, ICT/Media content analysis, public information and documentary material, Software development, Usable Security, P&SbD	State-of-the-art research, ICT/Media content analysis, public information and documentary material, Software development, Usable Security, P&SbD
Outcome	Main RS activities and activists using traditional channels and social media identified Understanding of the context (political, activism), activist ICT use and four needs (one of them: lack of structured approach to security and privacy)	Build technical design and prototype Cyberactivist, based on one of the needs from phase I. Obtain further feedback and specific requirements to improve the prototype	Status update on main RS activities and activists and their ICT use Three security and privacy issues for the activists Feedback and specific requirements from CHI researchers and international activists to improve the tool Further improved Cyberactivist (functionality, UI, issues)	Information on comparison with other geographies, activities, and activists Further feedback and specific requirements from CHI researchers and international activists to improve the tool Pyramidal threat model Further improved and published Cyberactivist tool with customization and localization options, and the answer to the threat model integrated. Open-source code is also shared.
Status	Published	Published	Published	In submission (planned JCSCW)
Section	4.1	4.2	4.4	4.3

Later we iterated this approach in the third phase of our research, to update the information about the activists and protest landscape and the ICT use.

The second objective of the first phase was to identify the prominent activists for the application of qualitative conversational techniques. Main sources of information here were, besides the participants of the above-mentioned activities, number of "mentions" in public broadcasting services, print and online media), as well as personal acquaintances of the author. After the identification we both "followed" the online and observed the offline engagement of these "high-profile" activists. These were either involved in local non-profit organizations or "boutique" media outlets in a full-time or part-time capacity, or with widely known international non-profit organizations. Fully independent activists who had a relevant impact in the mentioned activities could not be identified in the first phase, but that was the case in the third phase described later. NPO and "boutique" journalism have their unique relationship with the activism in the western Balkans. On one hand they offer certain resources and on the other hand they are able to acquire and/or incentivize intellectuals interested in activism and society. Many activists are connected through nonformal means and some of these groups remain active as (in)formal citizen initiatives. Although some activists do not involve themselves in open political discourse, most of them directly criticize the national or municipal authorities. Due to this fact, parts are even "branded" as „traitors" and „provocateurs" by some stakeholders, their access to public funding and media outlets is limited and they are frequently sued. Activists propagate information about the activities and their ICT use primarily through recommendations, social media, and quotes in oppositional media, correspondence, and posts. Here again the "snowballing" techniques were helpful to obtain the information on other activists which were missed in the observational part. A full list of the activists, as well as the format and the timeframe of our engagement with them is available in the following sections.

The third objective of this phase was to engage the prominent activists, to qualitatively complement the results of the applied observation techniques.

We prepared the following "package" before we approached the activists (Annex I)

- Letter signed by the researchers and introduction, explaining the topic of the study and the intentions of the researchers,
- Questionnaire,
- Note of the participation and recording consent, pseudonymity, and non-disclosure.

Around three quarters of the activists contacted by the author accepted to participate in the conversational part – mostly those engaged in the "Save the Park" initiative. These are listed in Table III in Section 4.1. We focused on in-depth, semi-structured, qualitative interviews based on the model similar to those described in Küsters (2009), Witzel (2012), or Gee (2014). One interview was conducted in person in Banja Luka using the digital recording app on the smartphone, others remotely using Microsoft Skype extended with plugin Skype Auto Recorder.

Interviews started with a description of the research and the rules on anonymity, and data protection of the recordings. Then the name, organization, position, activism experience, birthplace, birth year and workplace of the activist was documented. Two stimulus questions were asked and where necessary, up to 40 questions were asked in addition regarding their ICT use practices and challenges, then inclusion of technology in social-political practice, and finally development and optimization potential of their ICT. The activists have not received questions in advance, and we also steered the dialogue based on interests our respondents showed (see e.g., Helfferich (2009) and Küsters (2006)).

In interviews conducted between February and October 2014, approximately 500 minutes of audio were recorded in the languages of the western Balkans. Audio records in MP3 format of all interviews are securely archived by the authors. The more than 100 pages of transcripts in English were made by a freelance student and Microsoft Word, with adaptation of the local slang terms.

In the next step, all of the answers relating to the ICT were extracted from the transcript and clustered according to the topics (e.g., tools used, privacy and security remarks, negative experiences). They were then prioritized based on keyword frequency and the quality of the insight (one of the paper authors has extensive practical background in security and privacy). From that, authors described the fundamental issues and developments of the ICT use by this group. The findings pointed out the fact that security and privacy aspects may play a vital role for the ICT use by the activists, but also for their general safety and wellbeing, as described in detail in Section 3.2. The authors decided to pursue a technical design that might support these efforts.

As the activists are fragile group working in a sensitive environment, the authors took precautionary measures during the research process, orientated towards the ISO 2700x standard. The data handling and the "anonymization-before-publication" procedure were

communicated to all participants. Physical interviews were implemented in a minimum risk environment e.g., in safe environments such as public parks. For online interviews, unencrypted Skype was used before 2018, but with an assumption that RS or BH authorities were not able to maintain surveillance, and afterwards replaced with end-to-end encrypted WhatsApp after 2018. All audio files, transcripts and notes are archived on the encrypted drive of the author.

3.2 Phase Two

The research questions which dominated the phase two was: how to design an effective tool that on one hand raises the awareness and levels of privacy and security, and on the other hand, be available, usable, and attractive to the activists with relatively weak hardware, low ICT know-how and low awareness for the topic.

Let us highlight that our social media monitoring, as described above continued during all phases of our research. It was less intense, but it continued to provide valuable data about the activists and the activities in the region (e.g., frequency of the social media site "sweeps" or logins was reduced to monthly). E.g., the monitoring enabled us to identify Kevin or Alena as the engaged activists which we did not know in the first phase, but which were happy to participate in the test of the tool described below.

The development of the prototype of the web application "Cyberactivist" took place between July and December 2016, using HTML 5, JavaScript, and CSS. The dissertation author has written the whole source code of the initial version. Co-authors of the paper in Section 4.2 also tested and provided feedback regarding the usability and functionality. The application user interface was offered in English and Serbo-Croatian language. Then we shared a link to the prototype with the selected activists from both phases per e-mail. We did not provide the participants with any information besides that the tool is focused on privacy and security. We also informed them that neither usage data nor answers to the self-test questions were transmitted to the authors during or after the test. All of them tested the application in one day and spent with it several hours of their time. Most of them, according to their own account, were checking out the tool sections, filling out the self-test and following the links the tool suggested based on the test outcome.

We then conducted an interview with the activists in the Serbo-Croatian language to document their experiences with the tool and its possible improvements. We digitally audio-recorded four hours in five separate Skype sessions with the recording plug-in between May

and September of 2017 and one activist complemented his short audio statement with an e-mail. The key findings of our interviews were transcribed in English language and comprise approximately 50 pages, elaborated in detail in the Section 4.2. Besides direct ideas, the learnings from the interviews inspired the authors, which then also generated further ideas on how to improve the tool, such as better user experience, a more intuitive user interface and adding current information sources.

It is important to emphasize that our interviews had two facets: we asked for their feedback about the tool, as described above and in Section 4.2, but we also asked them what changes they observe in the RS and social media environment. These inputs were "saved" and merged with additional inputs for the phase described in the next section.

3.3 Phase Three

Phase three of our design case study focused on the following questions:

- How did the activism, and related use of ICT / social media in RS, a very fragile post-conflictual society, evolve since the first phase of our research?
- What are the critical issues regarding security and privacy aspects of social media use among RS activists?
- How does Cyberactivist tool evolves to be effective and usable in addressing these issues?

As mentioned in phase two, we continued to apply observational techniques to identify changes within activist landscape and their ICT and social media use. We added some new sources to our "following" which appeared after the initial observation (e.g., television channel BN, its portal and social media appearance as an opposition "counter pole" for authorities' public broadcaster RTRS which also further developed its social media presence). In this phase, beside observation of the dynamics of the RS cyberspace, our observation focused on anonymity, privacy and security aspects related to activists. Based on selected criteria (e.g., own post vs. repost, offline reaction during the protest), prominent actors were further observed or invited for interview follow-up. Most posts were in the western Balkan languages, but also occasionally in English or German. Posts contained texts, lyrics, songs, live streams, videos, photos, illustrations, memes, and links to posts from other platforms. This analysis between January 2016 and April 2018 produced approximately 60 hours and 40 pages of (partially handwritten) notes.

We conducted two types of interviews in this phase: with the (for us "new") activists and with CHI researchers in the area. Both groups provided feedback regarding the user experience and

functionality of the tool Cyberactivist, while the activists additionally provided feedback on the changes in the RS and their ICT use.

We contacted all the RS activists from the first phase and the "new" activists. Seven of them responded to our invitation, with two from the first phase of our study. Most of them were actively engaged in the "Justice for David" campaign. Our interviews during were like those in the phase one, consisting of the same elements (e.g., data protection disclaimer) and again, semi-structured in that the questions included some topics we had already evolved, esp. related to their experiences of Cyberactivist tool. Broadly the talks were mostly focused on changes in their ICT infrastructure and use. We paid attention to the challenges, security and privacy aspects, inclusion of ICT in social-political practice, and potential development and impact optimization. In parallel and analog to phase one, we let them share any relevant topics with us ("freely speak"). This time, approximately five hours of material were audio-recorded using Skype with audio recorder option and WhatsApp between May 2017 and October 2018. One activist provided an e-mail response in addition to his statement. The interviews were transcribed and translated, producing approximately 60 pages. In addition, we wanted to cover the full scope of possible threat to the activists; as RS at the time did not have any significant recorded cases of aggravated assaults or on-going conflicts with activists, we interviewed one Lebanese activist in June of 2018. We again clustered all of the answers according to the topics (e.g., used tools, privacy and security, experiences) and prioritized them based on frequency, but also insight quality (from the perspective of security practitioner). From the main changes and issues were extracted, as well as the threat pyramid described in Section 4.3/4, as well as further ideas for the improvement of Cyberactivist.

In order to make the tool transferable into other activist environments, we decided to approach another group of stakeholders. The author conducted a workshop with researchers in the domain of CHI, having well versed in the design case studies and understanding of the needs and privacy/security situation of the activists from Africa, Asia, South America, and Europe. Again, all activists and CHI researchers were told only that the tool is web based and focused on privacy and security awareness. The workshop was organized as a semi-structured, non-recorded, 3-hour-workshop session in May of 2018, complemented with e-mail feedback. To achieve better comparison among the Balkan countries and check the wider applicability of our findings, an interview with a researcher in the Solidarity movement in 2018 via Skype produced further recording. These formats produced over dozens of requirements which led to technical and content changes within Cyberactivist.

3.4 Phase Four

In the last phase of our research, leading to the publication of this dissertation, we considered three major sources:

- the feedback obtained from the CHI/CSCW research community during the review of our papers
- insights obtained from the comparison with other regions where activists are facing similar challenges
- comparison with other available similar non-profit and commercial tools in the domain of security and privacy awareness.

The feedback obtained from the research community helped us establish a better structure and provided hints on both specifics of the Balkan region as well as possibilities to globalize the conclusions of our study. It also allowed the authors to sharpen our research contribution and increase usability and attractiveness of our technical design. Insights from the other regions help us to weigh the risks and distinguish anecdotal evidence from the general claims. Comparison with other similar tools helped us to identify the unique features of Cyberactivist and provided hints about the optimal publication, configuration, and customization method. As a result, it led to the new globalized version of Cyberactivist which was published on the web platform and repository Sourceforge.net and independent website hosting service. The study participants got information about the updated version of the tool, and we promoted Cyberactivist on various traditional and social media.

3.5 Involved Socio-Political Activists and CHI Researchers

As described in the previous section, we involved numerous activists and CHI researchers to provide feedback on the situation and findings, formulate requirements and perform friendly user tests of the tool. They are listed in Table II under pseudonyms.

The letter A in the column Type marks the activists and R the researchers. Annexes in electronic format that follow this document hold related files and templates.

II: Interview Partners and Feedback Group

#	Pseudonym	Sex	Birth-year	Location	Type	Role	Contact	Form	Feedback
1	Brad	M	1980	Banja Luka, RS/BH	A	Project Manager at RS NPO, 2006	03/2014, 05/2017	Online	Interview, 200 Min
2	John	M	1978	Banja Luka, RS/BH	A	Public Relation Officer / Editor at local NPO	02/2014	Online	Interview, 93 Min
3	Olivia	F	1988	Banja Luka, RS/BH	A	Deputy Editor at local NPO / online magazine	06/2014	Online	Interview, 56 Min
4	Anna	F	1988	Banja Luka, RS/BH	A	Project Manager at the local NPO	10/2014	Offline	Interview, 71 Min
5	Grace	F	1958	Banja Luka, RS/BH	A	Head at the local branch of an international NPO	10/2014	Online	Interview, 72 Min
6	Ela	F	1984	Banja Luka, RS/BH	A	Project Manager at the RS branch of an int. NPO, 2008	04/2014, 09/2017	Online	Interview, 93 Min
7	Adam	M	1981	Den Haag, Netherlands	A	Individual activist of RS origin, EU citizen and home	09/2017, 11/2018	Online	Interview, 24 Min
8	Kevin	M	1981	Banja Luka, RS/BH	A	RS journalist / an individual activist	09/2017	Online	Interview, 76 Min
9	Alena	F	1980	Banja Luka, RS/BH	A	Individual RS activist for disabled population	09/2017	Online	Interview, 30 Min
10	Peter	M	1969	Banja Luka, RS/BH	A	Individual activist (leader) from RS	06/2018	Online	Interview, 32 Min
11	Lepa	F	1985	Vienna, Austria	A	Individual activist of RS origin, EU citizen and home	11/2018	Online	Interview, 40 Min
12	Ali	M	1984	Bonn, Germany	A	Individual Lebanese political activist	05/2018	Offline	Interview, 20 Min
13	Stavros	M	-	Siegen, Germany	R	Researcher of Greek political activism	09/2018	Online	Interview, 29 Min
14	Haras	F	-	Siegen, Germany	R	Researcher of international political activism, e.g., Morocco	05/2018	Offline	Workshop, 180 Min
15	Daner	F	-	Siegen, Germany	R	Researcher of international political activism, e.g., Palestine	05/2018	Offline	Workshop, 180 Min
16	Omit	M	-	Siegen, Germany	R	Researcher of „usable privacy"	05/2018	Online	E-Mail
17	La	M	-	Siegen, Germany	R	Researcher of international political activism, e.g., Syria	2013-2020	Offline	Workshop, 180 Min
18	Siega	F	-	Siegen, Germany	R	Researcher of int. political activism, e.g., South Sudan, Uganda	05/2018	Offline	Workshop, 180 Min
19	Cloude	M	-	Siegen, Germany	R	Researcher of int. political activism, e.g., Tunisia, Columbia	2013-2021	Online/ Offline	E-Mail, Talks
20	Trademark	M	-	Siegen, Germany	R	Researcher of international political activism, e.g., Iran	2013-2021	Online/ Offline	E-Mail, Talks
21	Soiram	M	-	Siegen, Germany	R	Researcher of international political activism, e.g., Middle East	05/2018	Online	E-Mail
22	Evad	M	-	Siegen, Germany	R	Researcher of international political activism, e.g., Europe	2013-2021	Online/ Offline	E-Mail, Talks
23	Tol	M	-	Siegen, Germany	R	Researcher of international political activism, e.g., Europe	2018-2020	Online/ Offline	Talks

4 Publications

4.1 ICT Use by Prominent Activists in Republika Srpska

4.1.1 Abstract

Bosnia-Herzegovina and its administrative unit or "entity", Republika Srpska are divided, transitional post-war societies. The aim of this paper is to present a preliminary analysis of regional activists' use of information and communication technology (ICT) and to identify improvement potential. Empirical investigations of social media use and qualitative interviews with the country's activists indicate strong interest in ICT. Benefits for the use of ICT by activists include more efficient access to their target group, easier information sharing with the general population, and quicker reaction to spontaneous "offline" activities. Simultaneously, data points to problems such as limited budgets and know-how, intensive outsourcing practices, and a significant lack of awareness regarding data security. Activists see improvement potential in areas of training on content optimization, campaign management, ICT use and maintenance, security, and privacy. Additionally, there is potential to improve upon the sustainability of activist's work and patterns related to their ICT outsourcing.

4.1.2 Introduction

ICT use in social and political activism has been an important topic for CSCW/CHI research community in recent years. Selected examples include Mexican Urban warfare (Monroy-Hernandez 2013), the "Tunisian spring" (Wulf et al. 2013), the Ukrainian war (Ronzhyn 2014), and activism in Palestine (Wulf et al. 2013), Egypt (Al-Ani et al. 2012) and Iran (Rohde 2004). It has been suggested that examining the socio-technical factors that produce political activities in their specific forms might be thought of as "Conflict IT". Such a proposal requires us to do rather more than to produce case studies of activist or other political practice, however, but also to contextualize those practices in some way - to place them in a context which, for instance, describes the relationship between the State and civil society; the infrastructural features that limit or afford possibility, and the intermediate channels and/or institutions that facilitate the formation of "publics" (cf. Dewey & Rogers 2012). This paper focuses specifically on the former Yugoslavia, which is now comprised of a number of recently formed independent states. One of them, Bosnia-Herzegovina (B-H), has experienced several major protests in the previous years. The country consists of two parts or "entities", as defined in General Framework Agreement for Peace in Bosnia & Herzegovina (1995) and Ustav Bosne i Hercegovine (1995): Serb-dominated Republika Srpska (RS, 2013

population of 1.3m living on 25,000km^2, major city Banja Luka) and the Muslim-/Croat-dominated Federation of B-H (FBH, 2013 population of 2.4m living on 26,000km^2, capital city Sarajevo). B-H still faces significant challenges after the bloody Yugoslavian conflicts of 1991.-1995., the most relevant being (European Commission 2014):

- no overall political alignment on the future of the country
- a slow post-war reconciliation and re-integration process
- a high-level of unemployment, corruption, and emigration.

The State, in this context, is experiencing a transition from socialism to capitalism, from a one-party system to a more democratic form and lacks overall legitimacy. The region remains volatile. Civil society remains fragmented and lacks an overall consensus about future direction. It is further bedeviled by social and economic problems of a very serious nature. In this dynamic and unstable environment, political activism takes on, we argue, a particular flavor. This paper presents results from the first phase of a multi-year, qualitative, exploratory, and participative research which deals with political activism. Our goals were to a) identify the main protagonists involved in activism in RS within last decade, b) review practices of prominent activists in RS in regard to their ICT use (esp. social media) and c) over time, and together with them, identify tools and practices which can improve their efforts in the future. In the next section we describe the current socio-political context in B-H/RS and summarize research on regional activism, the non-profit sector, and their ICT use. Subsequently, we analyze the state-of-the-art on ICT use in international non-profit organizations (NPOs), and thirdly describe research into social and political activism. We then, fourthly, describe our qualitative content analysis and semi-structured interviews. Section five contains a discussion of our research results thus far, pointing out major challenges that activists face in this context. The last section reflects on possible and requested tangible support for regional activists.

4.1.3 NPO Sector and Activism in B-H/RS

The fostering of intensive communication among diverse ethnic and social groups in B-H is one of the necessary prerequisites for addressing some of the country's challenges. The Internet and the use of social media offer opportunities to promote this type of interaction. In B-H, there are 2.63 million Internet users (penetration factor 67.9%) and 1.35 million Facebook users (Internet World Stats 2015). Social media, including Facebook, Twitter, forums/micro-blogs on popular websites, and Youtube, are increasingly used for political and social discussions and activism. The ability to react quickly to major events, provide

independent opinion to citizens, and multiply the impact of activism has been facilitated by high cellular phone penetration (>87.7% in 2015 (Business Monitor International 2015)), esp. smart phones with camera and media sharing options. Local Internet content is not formally censored by the authorities and is therefore a preferred medium for expression of any discontent. We were specifically interested in the role of ICT and social media because they play a "critical role especially in light of the absence of an open *traditional* media and a civil society" (Khamis & Vaughn 2011). Our research questions related to so-called cyber activism (Howard 2011), "the act of using the internet to advance a political cause that is difficult to advance offline". While the social media may provide a vehicle for dissent and for mobilization, such a role is not guaranteed. In January of 2015, the Government of RS proposed a new Law on Public Order to the RS National Assembly. This law defines social media as a public place and as such, offering possibilities for "organized public disorder activities, such as physical attack on persons… or property". It defines fines or prison sentences for such conduct (Republika Srpska Ministry of Internal Affairs 2015). The proposal initially produced some understandable trepidation among activists, although there has, at the time of writing, no obvious reduction in the quality or quantity of online content. RS also does not have formal strategy for engaging with the social media (cf. with Russia's approach according to Meredith 2013). According to Delegation of European Union to B-H (2014), after the war in B-H there was *"an explosion of non-profit organizations (NPO). However, this 'explosion' is of quantitative rather than qualitative nature. The country's *administrative* entities do not have a strategy for cooperation with civil society. At present, there are nearly 12,000 organizations registered in B-H. However, estimates of active NPOs range anywhere from 500 to 1,500. Of these, a significantly smaller number could be described as 'professional organizations'. The NPO sector is challenged because of 'donor driven image', lack of communication with the governmental sector, poor communication within NPOs, non-transparent distribution of domestic funds aimed at NPOs, and perception of political influence on some NPOs."*

It is clear that, in this country, social media and Internet use have "not been fully implemented in the field of political communication …, or at least it has not been implemented properly … except in the case of NPOs" according to Turcilo (2010). Barakovic (2011) explores the potential of Facebook activism to start "Arab spring" type of revolutions in B-H and claims that "anti-government protests via social media introduced a new phase of cyber activism in B&H", but nevertheless "reflected the latent character of the general public". His conclusion corresponds to Rosenberg (2011), who argued that Egyptian activists copied practices from

activists in Serbia (B-H/RS neighboring country) and “showed the limits of social media for democratic movements: Facebook attracted many sympathizers online but was unable to organize them well offline”. In B-H/RS, “grassroots activists have begun mobilizing around unemployment … Many signs during the latest protests also featured slogans related to corruption in hiring, and particularly with government employees (including parliamentarians themselves)” (Kurtovic 2013). However, the same author notes that “during a meeting of the organizers, someone stated that protesters cannot hope that those thousands of people employed by the State will ever rise up against it—suggesting that the current political economy may be curbing rather than inspiring civic revolt”. According to Armakolas & Maksimovic (2013), the June 2013 “protest against the government's failure to adopt the Law on the Unique Citizen Identification Number…, which media have called ‘babylution’… represent for some the largest and most significant example of social mobilization in B-H post-war history”. It adds that “a certain feeling of solidarity and compassion unusual for the deeply divided society was widespread throughout the country, irrespective of entity boundaries and ethnic differences. By sharing information about the protests, their peaceful methods and civic orientation, the social media played an important role in this process”. Numerous social media sites were quoted by Jonjic (2014), who claims that “with the current protests things were set in movement, which the country cannot reverse. If citizens show endurance and beyond ethnicity jointly criticize, this will mean, if not ‘B-H spring’, then ‘spring awakening’ for B-H”. In RS, these protests were also supported by a symbolic part of the population and limited in public display and gatherings. On one side, there was a fear by RS citizens that solidarity with FBH protesters may be interpreted as identification with the other entity’s assumed motive for degradation of the institutions of RS. On the other side, there is also the fact that the RS government quickly produced a temporary legal frame for solving this issue for its citizens, which was not the case in FBH. In sum, there are doubts about whether, in the current unstable and divided situation the social media have any power to transform socio-political reality. Conversely, and as we shall see, social media seem to be closely linked to political and social developments elsewhere. Our research, then, focuses on ICT current use in relation to socio-political activities in RS and the intermediate status of its transition to a stable state. One of the paper’s authors has origins in the region and Serbo-Croatian language as his mother tongue. Through this, a network of activists could be more easily identified, accessed, and interviewed. RS is also more homogenous compared to the complex entity of FBH, with more dispersed activists in 10 cantons.

4.1.4 Related Work - in International Context

In order to draw parallels with this country's situation, we looked at related state-of-the-art research on ICT and social media use in (a) political uprisings, (b) within international NPOs, and (c) in the context of civic participation.

4.1.4.1 Social media use in the context of political uprisings

Many developments in RS/B-H support the thesis that "social media systems together with mobile phones may well play an increasing role in political uprisings" (Rathi et al. 2014) Also, there are numerous similarities to the Tunisian situation (Rathi et al. 2014) where "social media linked the young activists with actors" and "allowed organizing resistance". Facebook, as perceived by Tunisian Internet users had political, informational, and a media platform role in the Tunisian revolution (Marzouki et al. 2012). Activists' groups in our case are similar to those described by Wulf et al. (2013) (e.g., volunteer setups, the ad hoc nature of organization, and limited financial and technical resources). Therefore, "nomadic" knowledge sharing practices from the European Social Forum (Wulf et al. 2013; Saeed et al. 2011) have also informed our understanding of activist cooperation in temporary protest groups (e.g., among student protesters who met only for one specific protest occasion in 2013). Khamis & Vaughn (2011) summarize that "communication revolution has succeeded in providing people in the Arab world with new 'weapons' to engage in their simultaneous political and communication struggles against their authoritarian regimes and long-time dictators, namely: their cell phones and computers", enabling them, "to exercise their agency and capabilities, empower themselves, and mobilize their public will". In the same manner, the author asks "if they will be equally successful in using them to win their ongoing battle to achieve a swift, safe, and smooth transition to democratization". The same 'weapons' are being used by RS activists. Al-Ani et al. (2012) make similar observations and provides examples of blog and social media utilization under unstable conditions. What is less clear is what the role of the social media might be in social situations which remain unstable, but which are, so to speak, 'post-revolutionary'. This is exactly where specific RS situation analyzed in this paper contributes to CHI research body: the country being post-war, mildly unstable for years, but having full access to the ICT available to other Europeans.

4.1.4.2 Social media use in international NPOs

Research into NPOs is quite extensive, albeit in specific contexts. We were not, for instance, able to identify any significant body of work concerning ICT use by Southeast European /

Balkan NPOs. Reljic (2004) focuses on peace journalism and media-supported conflict resolution, as well as certain features of the traditional media which can influence new media use in B-H. ICT use in the environmentalist sector is discussed by Colakovic & Markic (2010) and Massung et al. (2013). We also discuss one environmentalist NPO in this paper. Beyond the Balkans, we identified several authors engaged with the topic of social media use in NPOs. NN/UN (2010) illustrates NPO ICT use in developing countries through numerous examples. Analysis of Lovejoy & Saxton (2012a) revealed three key functions of micro-blogging (e.g., Twitter) updates— "information, community, and action". Although the informational use of micro-blogging is extensive, NPOs from the United States of America (US) are better at using Twitter to strategically engage its stakeholders via dialogic and community-building practices than they have been with traditional websites. Their subsequent study (Lovejoy & Saxton 2012b) found that the largest US NPOs were not using Twitter to maximize stakeholder involvement. Instead, they continue to use social media as a one-way communication channel. Less than 20% of their total tweets entail conversations and roughly 16% demonstrate indirect connections to specific users. Nah & Saxton (2013) examined organizational adoption, frequency of use and dialogue on Facebook, comments on Twitter and the use of social media in 100 US non-profits, and found that organizational strategies, capacities, governance features and external pressures all play a part in social media adoption and utilization outcomes. Waters & Lo (2012) performed a content analysis of Facebook profiles of 225 American, Chinese, and Turkish NPOs. This analysis showed that the global connectivity of social media, to some degree, is blurring traditional local boundaries in favor of the creation of a virtual international culture. Whether this logic of 'cultural homogenization' extends beyond this context is, as yet, unclear.

4.1.4.3 Social media use in the context of civic participation

Civic participation is, of course, a rather more amorphous concept. It can be applied to very specific engagements in small localities, as with Aal et al. (2014), where researchers analyzed Palestinian refugee camp application of the "come_IN" computer clubs. This "well-established approach to foster learning, social networks and integration in intercultural neighborhoods of Germany" from Stevens et al. (2005) may, of course, be applied on a wider level e.g., in B-H, if network infrastructures exist and can be successfully supported. The discussion on the possibility of implementing multi-span information systems in Rwanda by Yoo et al. (2013) also points to the challenge of sustainability - how various techniques, envisioned challenges and potentials can also be explored for long-term applicability (e.g.,

war crimes and repatriation, topics the Balkans are also facing). Jonjic (2014) provided an insight into the role of civic media curators, who acted as aggregators and disseminators of information via Twitter during the violent phases of Mexican Drug War – interesting to us because they are analogous to the unstable and unpredictable environment seen in B-H. In many Occupy movements following the Occupy Wall Street action, an example being Oakland, social media played a considerable role in connecting activists throughout the world. Using social media, *Egypt's* Tahrir Square protesters planned a protest to support Occupy Oakland (Skinner 2011). This kind of support we also saw in B-H protests, mentioned in the next section. Massung (2013) identifies the problem of using several social media in parallel, showing how movement to new channels can cause some confusion (e.g., updates on Youtube and not Facebook, leaving former users thinking there is no new physical activity on-going), as well by search engine ranking of the groups and posts. An interesting proposal is to use a "system that compiles information from multiple social media streams" and provide a comparison of "events on the Facebook pages of elected officials and police departments versus those of Occupy-related pages". The same author also discusses potential reasons for lows and peaks in the attention of social media users in relation to the protests, something we also observed in RS. Caren and Gaby (2011) claim that in the case of Occupy, "social networking sites have been critical for linking potential supporters and distributing information. In addition to Facebook pages on the Wall Street Occupation, more than 400 unique pages… and Occupy groups have recruited over 170,000 active Facebook users and more than 1,4 million 'likes'... Major uses for Facebook… include the recruitment of people and resources to local occupations, information sharing and storytelling, and cross-group exchanges. While the focus of Occupy Wall Street is on mobilizing individual's offline, online activities greatly facilitate these efforts". Social media contributed to "an emerging logic of aggregation", bringing together "masses of individuals from diverse backgrounds within physical spaces" and "led to sustainability of the #Occupy movements in a post eviction phase" (Juris 2012). It is easy, especially if we look at examples from the next section, to draw parallels with activism in RS. Although evictions from apartments illegally occupied during the war are almost finished, remaining evictions in the country still draw considerable amount of traditional media attention. ICT use by the activists during one eviction in the USA is provided by Asad and Le Dantec (2015), highlighting direct democratic engagement through information practices of situating, codification, and scaffolding. Our method, then, was predicated on the view that we wished to identify existing

activist practices and facilitate them in working more towards democratic principles, an explicitly participatory agenda.

4.1.5 Method

This paper presents the first phase of planned multi-year research, consisting here of an analysis of the communication practices of RS political activists. Design case studies and ethnographic action research (EAR), as described in Wulf et al. (2011) and Tacchi (2009) respectively, served as a basis for our research. We applied both in the firm belief that rich understandings of local conditions and needs will raise quality of later technical design and implementation. A mix of observational and conversational techniques was used to understand the major activities of recent years in RS and how activists use(d) ICT in pursuit of their work. During the analysis we read activist posts and event announcements, supporter and opponent reaction (e.g., comments, likes, sharing), speed and path of information spreading etc. This phase lasted from June 2013 to September 2015 and included two parts:

1) Identification of the main activities where ICT and social media were extensively used in recent years. Data was collected from RS-related contents on social networks (e.g., popular groups/pages on Facebook, Twitter, micro-blogs on Youtube videos, and popular websites) and prominent traditional media reports (such as State broadcasting services, magazines, and newspaper), identifying those issues which generated most traffic. Later we "followed" these prominent activities over a period of time (e.g., regularly reading news feeds) with a view to gaining a picture of their trajectory. Initial analysis informed us about the activist landscape and the major events they were involved in the recent years and enabled the inclusion of specific questions into our later dialogue with activists, both raising quality and improving our understanding of their answers. The activities in RS which had a high number of participants and most (esp. social) media attention were:

i. "Save the 'Picin' Park" (Park je nas 2015) – massive anti-corruption protests in city of Banja Luka in 2012 (Figure 5), triggered by the apparently illegal conversion of a city park into business buildings. Some of the activists faced trials for the activities mentioned above (and were initially convicted, though verdicts were later overturned). These activists were also supported from FBH, where citizens of Tuzla organized online support for Banja Luka protesters. Although protests lasted roughly one month, their consequences continued to ramify in 2015: the court sentenced a controversial businessman to three years in prison and a major telecommunication company cancelled the rent contract with the building.

5: "Save the Park" June 2012 Protests in Banja Luka, RS Largest City (Buka 2012)

ii. "Save the Castel" (Spasimo Kaster 2015) – a citizen initiative started in 2012 with self-organized, non-financed online support and the goal of raising awareness of the authorities' neglect of an ancient Roman fortress in Banja Luka

iii. "Citizen ID Numbers for our kids - Banja Luka" (Hocemo JMBG za nasu djecu 2015) – (part of "babylution" mentioned above) roughly 40-day long protests which occurred in 2014, following a parliamentary dispute preventing newborns from obtaining passports needed for e.g., international treatment.

iv. "Occupy Banjaluka" (2015) – activities following the Occupy Wall Street action in 2011.

v. "Floods in the region" (Poplave u region 2015) – social media activities around strong floods which hit RS in summer of 2014. There are several Facebook micro-sites founded for this purpose. All of them, including this one, continued to exist under the same name and same membership, but completely changed their scope after the events (e.g., to re-post various entertainment news).

Some of these activities began before our research had started. This meant that, as described by Salaheldeen & Nelson (2012), some information traces were lost although the quality of information obtained from the subsequent activist interviews filled these gaps (Salaheldeen & Nelson 2013), Social media activities related to iii and iv are minimal. On the other hand, i and ii are still drawing public attention.

2) Identification of activists, based on data available from the above sources, from media reports in RS (such as State broadcasting services, print and online media), as well as personal contacts. Later we “followed” the online activities of these “high-profile” activists.

Totally independent activists (without any organizational affiliation), who could be said to have had a significant impact in activities described above, could not be found. Activists were either involved in local organizations (such as a local environmentalist NPO with no subsidiaries outside of B-H) or with international organizations (such as branch of an international anti-corruption NPO). Of our informants, John, Ela, Anna and Grace are in a full-time working relation with their organizations, and Olivia and Brad are paid on a contractual, project basis (part-time). NPO has its unique set of relationship with B-H activism primarily due to the fact that they offer activists certain resources and that NPOs were able to acquire and/or develop critical thinking intelligence, interested in activism and societal change. Both established and less-known activist groups are connected during activities through non-formal means and have no joint “umbrella –organization” or legal form. Some of these organizations remain connected (e.g., in case of activity i or v), nevertheless, as informal citizen initiatives.

Activists in our scope are fighting corruption, nepotism, social inequality, and the indifference of politicians to everyday issues. Their sample slogans include “Cajavec, Incel… *ruined ex-state companies*”, “silence is in vain, it’ll be even worse #tuzla, #banjaluka”, “we’re all foreign mercenaries, our State is financed by International Monetary Fund”, “I’m sick and tired of ‘better’ life”, “Don’t touch, even the snow is owned by the *ruling* party”. Paper’s activists are middle class citizens, mobilized and non-violently active in both digital and physical environments. They are primarily motivated to use ICT to amplify their impact and fulfill information needs of public engaged in the events, which were provided limited or no space on traditional media (Egypt’s activists (Alexander & Aouragh 2014) had similar motivation). Although some activist groups do not involve themselves in overt political discourse, most of them are, even so, engaged in oblique criticism of the national or municipal government within the RS entity (independently of which political party is in power). They were often in the past 20 years described as „traitors” and „mercenaries” by government agencies, so a sense of threat has been constantly there. As “compensation” for having foreign budget support (e.g., from US embassy or headquarters in Germany), their access to public funds and media was limited. Activists a-e were described as “supporters of the RS destruction” and “foreign mercenaries” in a publication of the ruling party Karganovic (2014).

Some of them were convicted in the Banja Luka district court in February 2014 for supporting activity i. However, the verdict of the lower court was overruled after appeal in June 2014. These facts, combined with popularity and persistence of the activities, and legal prosecutions of the activists mentioned under i, suggests that our initial selection of activists and activities for further study was justified. Information was mostly propagated outside of the net through "word of mouth", social media, and quotes in oppositional traditional media, e-mail and blogs. The degree of persistence of their activities is described in the method section, where groups are listed.

The most prominent activists and NPOs, either involved in the above activities or continuing to have, in 2015, a significant number of "followers" in social media, are:

a. Buka (2015) – online/print magazine/TV show, which symbolizes critique of regimes, corruption, and nationalism

b. Center for Environment (2015) – an environmentalist NPO

c. Transparency International B-H (2015) – a branch of an international NPO

d. Helsinski Citizen Assembly Banja Luka (2015) – a branch of an international NPO

e. Friedrich Ebert Foundation B-H (2015) – a branch of an international NPO

f. e-trafika (2015) – one of the leading youth portals.

Our conversational techniques, as a part of EAR, were focused on in-depth, semi-structured, qualitative interviews, conducted with relevant activists from RS who have participated in the previously mentioned activities. Three other individual activists, identified during the observations of i-v, were also asked to participate in the study, however no response was obtained. Our approach to semi-structured, qualitative interviews was prepared as recommended by Küsters (2006), Gee (2014), Steinke (2000), Helfferich (2009), Krippendorff (2004), Mayring (2000) and Witzel (2000). Approximately 500 minutes of audio were recorded in six interviews with activists conducted between February and October 2014 in the Serbo-Croatian language (in exact order as depicted in the Table III). One interview was conducted in person, others remotely via Skype. Audio records of all interviews were archived, and transcripts were translated into English. There were minor challenges in translation such as local slang terms (e.g., "Picin"), none of them impacting the results. Transcripts amount to over 100 pages in English language.

III: Conducted Interviews

Pseudonym	Birth Year	Role / Active since	Duration ~Minutes
John	1978	Public Relation Officer / Editor at local NPO, 2009	93
Brad	1980	Project Manager at local NPO, 2006	140
Ela	1984	Project Manager at the local branch of an international NPO, 2008	74
Olivia	1988	Deputy Editor at local NPO / online magazine, 2006	56
Anna	1988	Project Manager at the local NPO, 2011	71
Grace	1958	Head at the local branch of an international NPO, 1998	72

Interviews started with a description to the activist of our research purpose, and policy on recording, anonymity, and data protection. In the second part basic data about each activist was collected: name, organization, position, activism experience, birthplace, birth year and workplace. Then, around 40 questions were asked regarding the state of their ICT infrastructure, use practices and challenges, inclusion of technology in social-political practice, and potential development and impact optimization of their ICT. The questions were selected because they enabled us to obtain tangible direct feedback on the ICT use of activists and to identify potential improvements. The activists have not seen questions in advance, although they had been informed about the general topic of the study and given rudimentary information about the intentions of researchers. "Snowballing" techniques were used to contact other activists where possible. Therefore, in each step, we aimed to iteratively reach more activists and obtain a more complete picture of the situation.

4.1.6 Findings and Discussion

As mentioned above, we explicitly asked activists what their major issues are and what ICT tools would help them in the future, which enabled us to rank the findings and potential improvements. We cross-referenced interview data with our observations from online content analysis and state-of-the-art. Initially, we merged the results into one list and removed the findings that did not seem relevant to ICT use. Then we weighted the relevant data on the list, according to the number of times similar statements were made interviews (e.g., several activists said "'like' is not as useful as person on the ground") and/or observed during the content analysis ("one Facebook post confirms specific activist's statement"). Then we marked elements already described in the state-of-the-art and focused on the new contributions. We ultimately grouped major findings into three categories based on their similarity: motivation and use of ICT, level of ICT competence, and security, privacy and anonymity aspects. Prospective improvements from the findings were also either mentioned by activists in our interviews or extrapolated by authors (e.g., simple cyber security control not known by activists). These were the need for specialized training, the implementation of security and privacy protocols, the optimization of self-learning/knowledge transfer, the

analysis of freelancer use and cooperation, increased ICT funding, and further best practice exchange with global activists. In order to define these groups, we ranked all improvement proposals, based either on the number of mentions by activists (e.g., “we would benefit from dedicated budget for ICT/training”), potential impact on their daily practice (e.g., need to backup data) or potential transferability to an international level (e.g., training for social media tailored for activists).

Motivation and use of ICT

The NPO and activist sector in RS/B-H is much more visible in new media than in the traditional media sector, while (pro)government mouthpieces are to be found inversely. This is confirmed by our content analysis of the social media and through statements like:

Brad: “…there is a rising use of Facebook and other social networks, but especially Facebook in this region… it allows us to inform people, transfer data fast and organize the events; either to go out on the streets, sign petitions, come to an exhibition or anything else without the fear of sanctions for the organization or for individuals because the law is still not treating social networks”.

From an activist perspective, the major qualities of social media, especially in combination with mobile devices are “time-to-audience” and reaction time (e.g., ability to publish first, followed by the rapid spreading of messages, allied to the possibility of direct feedback of affected individuals). Activists differentiate themselves and attract supporters through quick delivery of the actions and news; in comparison, major TV news broadcast “Dnevnik” at 19:30, followed by older RS citizens is, “slower”. Hence, Facebook is the default communication and promotion channel of/for the country’s activists. Facebook policy of “pay to increase post visibility” endangered some campaigns – it was easier to position a topic or coordinate the activities before that change (quotes from John, Ela, Olivia).

Olivia: “We have organized some events also via internet; …peaceful gatherings and protests on some public issues but it was also usually via some event on Facebook where we *were* invited.”

Authors believe that their impact can be further improved by skipping usage of public, “all-call” media, promoting deeper engagement with current and potential volunteers through interest matching via special platforms, which would need to be customized for RS (cf. Voida 2011).

Activist websites are present, but their effect is different from one activist group to another. Twitter and dedicated e-mailing lists, online apps (such as Dropbox) and blogs are also occasionally used. “Homebrew databases” as described by Voida et al. (2011) were mentioned only by Ela. This would roughly correspond to findings of Rathi (2014) and Wulf et al. (2013). One often heard statement was „no street - no change”: activities on Facebook and other online tools cannot replace activities on the ground (quotes from John, Brad, Olivia and Grace).

Brad: “It would be very good if there is a possibility for every *Facebook* like that we as organization get on every article or happening, we might also get a live person; a person that will translate his/her like, stand and expression of opinion to something concrete and practical in which that person is good at.”

Grace: “Our public is quite lethargic…split according to ethnic lines… except in cases such as floods, where these lines are crossed” (see flood group v in the method section)

Declared support on social media, such as the number of members or likes is always significantly higher than the actual offline support, confirming Rathi (2014), Rosenberg (2011) and Monroy-Hernandez (2013). Skype and Office tools are also regularly used by activists. Even so, the resources of most activists who participated in the study are very limited.

Anna: “Considering the internal state of infrastructure, we had this summer major issues with the computers that stopped working, one after another.”

Their primary purpose is usually project execution. All unplanned or ad-hoc activities, such as sudden citizen protest or appearance of new ICT tool are hard to support in terms of time, budget or people management. Increased ICT budgets would help to better empower NPO/activists, promote their contents, and increase effects of social media and their transfer to the “ground”. Examples include increased bandwidth (e.g., websites are unavailable during protests due to demand, slow access during peaks means losing interested citizens - all three deepening the secondary digital divide as described by Zimmer (2003)), better quality hosting (more space for citizen generated images and videos), better tools (databases, content analysis), and maybe even a common licensed repository of “easy content”. One interesting output of our study is that „easy content” attracts attention where focused content fails (e.g., on an activist site: images of “cute pets” to raise awareness for protest campaign). We also

identified a trend for hardware and software sharing, also referenced within the "community informatics" (Gurstein 1999):

Anna: "We often lend our laptops and equipment to other organizations… that have no equipment and offices"

A common hardware and software repository shared among RS activists would undoubtedly facilitate their work.

Level of ICT competence

The level of internal know-how in the ICT domain is characterized by limited resources, learning by doing, vague roles, the need for training, and extensive use of freelancers. Experience exchange on use of ICT with similar organizations in similar circumstances in Southeast Europe and worldwide would certainly contribute to improvement of ICT competence of activists in RS (comparable to transfer of activist experiences from Serbia to Egypt (Rosenberg 2011) or between Turkish and US NPOs by Waters and Lo (2012)). When starting the project, some activists had already considered initial training for resource planning, e.g., when a branch of an international organization introduces a database used in headquarters, there was a specific several months ICT training provided for the relevant branch employees. In some cases, participants brought some elementary ICT and social media skills when they joined projects and NPOs or started activist work. The other activists from the same organization sometimes tried to profit from that knowledge. In rare occasions project budgets provided the training in ICT, needed for everyday work and activities. Activist's need for training, especially beyond content management, is clearly communicated e.g.:

Brad: "…we need training regarding hardware equipment… software and managing websites".

Anna: "…additional knowledge in terms of use of … *ICT* infrastructure… social networks and internet in general… how we can communicate more effectively with our target groups. … lot of content on the social networks is being repeated; therefore, specific target groups put us on 'hide' and do not follow our content… it would be good to ask them what they are expecting from us considering the social network content so it can be a two-way communication; and not … bombarding *them* with the content that we think it could be interesting… Furthermore, considering that our target groups are marginalized - female

population, youth, and people with disabilities, maybe we should do surveys about their … social media usage so we can improve the quality of *our* content…"

In almost all cases, we identified intensive "learning by doing". Mutual support and knowledge transfer among fellow activists is present in almost all environments; but are particularly prevalent in technically simpler environments. "Newbies" are often supported by colleagues if they are encountering an ICT tool for the first time.

John: "Considering the internet knowledge, we are all self-taught… including the implementation of content-managing systems of *our* portal… we have just received the rules *of the system* by email and worked on it by ourselves".

Those who had available resources for introduction or exploration of new technologies at the right moment shared knowledge also with other organizations:

Ela: "some organizations … developed some great *ICT* platforms… *and* made revolution - they afterwards went around training *other NPOs on* … use of that new ICT".

If the technical know-how is not available, activists tend to research the problem on the Internet and find the solution. In some situations, activists were willing to take additional ICT training (e.g., on desktop publishing) and even change the focus of their duties in the organization to provide more value to their organization. Some activities were never completed due to lack of ICT competence (e.g., implementation of a much-needed "homebrew" cooperation database in Ela's NPO). Activists advise due care in balancing ICT introduction and sustainability:

Ela: "communication is overcomplicated and when you multiply the number of channels and profiles though which you communicate… we should not just jump into it until you weigh how good is that for the organization and … how much capacity there is for it to be sustainable"

In almost all organizations especially local NPOs and branches, only a soft distinction of roles is present: activists tend to be of "equal rank", meaning mostly having administrator privileges or non-limited accounts for content management of their sites, Facebook pages or Twitter accounts. The level of trust seen here is also discussed by Rohde (2004, 2007, 2013). Activists published and adapted content with limited, simple, and mostly implicit rules and permissions.

John: "…everybody does everything: administration of the website, comment approval, posting on Facebook."

Grace: "Some rudimentary roles are present, mostly decided by available *ICT* knowledge level."

Although social media eased content management and improved reach to target audiences, participants are still facing issues with development, administration, and customization of content. The attention span of B-H citizens, including those active via social media, seems to be very short. Therefore, activists see the need to be fast in achieving the goals of their communication before mass attention attenuates.

Some activists face challenges if their contents are discussed. The positive effect of their primary message being read by many citizens may be lost through too many discussions on social media (i.e., comments below a post). Comments occasionally distract from the primary goals set by activists (e.g., unrelated corruption comments on posts about ecological activity) or produce "hate language". The absence of a developed and consensual civil society means that offensive and often unrelated ethnic/religious hate comments are much more common than when compared to the rest of the Europe (e.g., music video commented on by nationalists purely due to name of the singer). Of course, internet trolling is a very well-known phenomenon, where anonymity encourages a sense of impunity and freedom from being held accountable for inappropriate online behavior (Hardaker 2010). Trolls in this particular case, however, are seldom constrained by any socio-legal framework:

Anna: "there is a lot of space for misuse… information not being verified on the Facebook… if somebody shares something about us, nobody checks with us the credibility of the information but quotes that source that posted it."

Grace: "*border between freedom of speech and spread of hatred and intolerance in B-H is very thin*…*and it's often crossed on social media*… sometimes I get sick from reading them – it's continuation of war by other means"

Due to trolling, some comment boards / forums are then either blocked or need a disproportionate amount of administrative effort from activists which published them. Social botnets such as those described by Hegelich (2015) used for trolling in the Ukraine have not been visible on RS Internet.

Although the level of ICT competence of activists is limited, it is not easy to compensate for it. Modest, mostly project-based funding and staff does not enable the opening of permanent positions for ICT experts in activist circles.

Ela: "…most of the NGOs are facing the problem of lack of expertise *and* resources" / "*it would be great if we would* have somebody inside of the organization that is an expert in … web design, technology…" / "…we have too many projects and too few people and then it is unreal to expect that we can deal with *ICT, social media, etc.*"

Anna: "we do not have internal capacity to hire *graphic* designer and web *creator* because it costs us too much."

Beyond tools such as Office, e-mail clients, web browser and Skype, almost all complex ICT services are outsourced to volunteers or relatively non-expensive young freelancers periodically engaged on an as-needed contractual basis. Web/system administrators and graphic designers are often the roles which are externally fulfilled. Research on the outsourcing practices of NPOs, where objectives for outsourcing are typically politically driven, is rather scarce. After their analysis of 200 publications, Kremic et al. (2006) claim that freelancer use and ICT outsourcing practices in the NPO sector provide significant space for further research. Our interviews shed some further light on the challenges and needs in this domain. Temporarily finding more volunteers with ICT background to help RS NPOs will be a "surface solution" (Voida 2011) and might be achieved through matching platforms (Voida et al. 2012). However, sustainable models for dealing with outsourced staff reacting to changes in the surrounding ecosystem, as well as permanent and cost-effective engagement with ICT and social media specialists in RS needs to be found. As in the case of HMIS (Le Dantec & Edwards 2010), the ability to customize tools would require a high degree of technical sophistication at the local scale (where on-going and unique reconfigurations have the most potential benefit, but where such expertise is least likely to be found). These resources might also be shared/co-financed among organizations, as specialist knowledge may not be needed all the time and is often related to peaks such as spontaneous protests. Furthermore, their portfolio can be standardized in domains where activists have similar needs (e.g., customization of content management systems). Freelancers might be partially used as trainers, due to their extensive ICT knowledge. Application of models such as those from Massung (2013) would provide better means to motivate more volunteers in this domain. However, non-screened volunteers and freelancers may also pose a security risk.

Status of data security, data privacy and anonymity

Answers to our questions clearly pointed to low data security and privacy protection levels as issues for the systems of the activists and NPOs. Activist groups occasionally face hacker attacks, and unfortunately no confidentiality, integrity and availability of data is ensured. In rare cases, data archiving and backup is applied. Channels and data being used are not encrypted, which can lead to communication interception, content tampering and anonymity breaches. Anonymity, secured via ICT controls, is very important in the context of RS activists. Pressure is sometimes exercised by people close to government, the ruling party or those affected by a specific activist's activity. Even the NPO sponsors, such as stakeholders from the western hemisphere, sometimes exerted pressure in certain situations (e.g., removal of an associate due to a critical website article). Also, from the perspective of some activists, "auto-censorship" (i.e., fear of consequences) is an important obstacle for the expansion of the activities.

Brad: "What we saw is that there was energy in people, although many of them stayed in the domain of only sending an email, *message* via their Facebook profile because there is a great fear, big auto-censure of people who say anything or express their opinion".

In addition, activists are susceptible to the compromising of their communication channels e.g., distributed denial-of-service attacks in key moments such as protests. There were statements regarding the presence of malicious software in systems, showing activists are susceptible to the challenges which every ICT user faces. However, there is a potentially larger impact due to the value of the data on these systems. At the same time the low awareness level of activists is broadly comparable to the low awareness level of the citizens in the Balkans:

Brad: "I doubt that we will have some hacker's intrusion … because the topic is still not so 'popular' in this country".

Targeted hacker attacks were limited and only relevant to one part of the activist community. Participants speculate that hacker attacks are triggered either by random international attackers (attack as on any ICT user, e.g., malware), or by someone instructed by a party engaged by activists in some controversial context (e.g., hacker paid by corrupt politician).

Ela: "We had attempts of hacker intrusions on our website"

Grace: “Some of websites… are hacked... there are occasional… or continuous attacks for a couple of days… we speculated whether they have political background”.

This topic is increasingly important, as the domain of ICT becomes more regulated here in the future (Karganovic 2014). Revised RS law on public gathering extending to social media produced numerous negative comments from activists on social media in the first quarter of 2015. Facebook policy has caused anxiety and concern (as one anonymous user put it: “let’s all curse on Facebook while we still can”). Having said that, at the time of writing, there is no direct evidence that these concerns reflect a deteriorating situation. Rather, they reflect a continued distrust in an embryonic State. There has been one, widely publicized case where a terrorist attack by an Islamist on a policeman in Zvornik resulted in both being killed. An RS citizen sympathized with the attack in his Facebook post was arrested and his ICT equipment taken (Banjalukain 2013).

Implementation of security and privacy measures in NPOs from basic awareness measures to technical controls (e.g., encryption or backup) would be highly recommendable but is, as yet not realized (Hoy and Phelps 2008). In the domain of political activism, this need is even more present. Prominent RS political activists regularly mentioned security, privacy, and anonymity issues in our interviews. Whether or not their concerns are justified, activists have a considerable fear of possible consequences and are careful to avoid public statements which are too controversial. Implementation of technical controls would minimize the risks of data being lost, stolen, intercepted, tampered with, and misused. It could also prevent technical support being unavailable during critical moments, such as protests, due to availability attacks. Securing anonymity and full identity protection of the informants would, we feel, be beneficial. Many of the topics we identified above involve allegations of serious corruption or suspicions about State behavior. While this might equally be true in more stable societies, the potential ramifications for activists in RS are more consequential.

4.1.7 Conclusion and Outlook

For prominent RS activists, social media content management is a crucial means by which access to citizens and other activists is made available. This takes place, as we have seen, almost entirely through Facebook; Twitter and other social media are rarely utilized. Our activists are digitally very active and consequently ICT-literate – they indeed need less training than “non-digital” activists. At the same time, they are largely self-taught, being neither ICT-professionals nor “digital natives”. Their skills are quite specific to their immediate experiences and can still be improved. Activists are motivated to educate

themselves on ICT matters on their own, provide a great deal of informal mutual support (within their own groups and across a wider community) and solve problems together when everyday routine activity allows it. The atmosphere of trust among activists enables soft role distinction and fairly effective rationalization of their very limited resources. However, an advanced ICT knowledge base (e.g., on new hardware, system and web development, administration and maintenance tools, and advanced features of social media) does not exist. Even if basic ICT knowledge was available, the competence necessary to reach and mobilize their target groups, while enabling security, privacy and anonymity still appears substantially out of reach to activists. A dedicated training plan and its execution in domains of basic ICT (desktop and mobile hardware, operating system, middleware, Internet, office, and communication tools) and social media would tackle the problem of currently missing in-house competence. Training to achieve better reach of target group and to improve handling of trolling would also be critical steps in advancing their work. It would lead to competence building in the organization, reduced need for external associates and optimization of their activities in regard to efficiency and effectiveness. Such training, of course, should be tailored to the specific needs of the activists, and tested considering their previous, possible, and planned activities. Optimally, trainers should be specialists with an ICT, regional and activist background (examples of "training customization" are visible from NN/UN (2010)). It is therefore important to design technology that can easily train activists not only in RS but across the world (Massung 2013). The issue of providing an appropriate pathway for potential activists and other concerned citizens to learn both the communication and negotiation skills, and the technical wherewithal, is a vibrant one and is made especially problematic given the severe lack of resources, and the constant fear that the State is not making desired progress to a more stable situation.

Elements which support specific knowledge transfer within the specific setup of RS activist organizations, as well as among RS and B-H activists and activist groups' needs further investigation. We know relatively little about the way in which political entities undergoing the slow process of "normalization" after periods of warfare or other unrest, and how the relations between the embryonic State and an as yet uncertain and divided civil society can be managed. The social media evidently play an important mediating role in this relationship but helping activists maximize their opportunities to exploit possibilities is a non-trivial exercise. There are certain elements of "nomadic knowledge artifacts" that would further help RS activists optimize "learning by doing" and self-learning (Wulf et al. 2013): member-centered communication spaces, topic-centered communication spaces, repository approaches, and

social mapping tools (e.g., self-learning knowledge/document repositories or systems like CHIC from Stevens & Wiedenhöfe (2006) or volunteer interest matching systems like VolunteerMatch from Voida (2011)). These elements would further improve the reach of activists, foster trust and coherence within organization and optimize their everyday activities. The means needed to ameliorate the state of affairs are not currently available, e.g., funding for permanent engagement with ICT experts or specialized training. All complex topics are therefore outsourced, mostly to freelancers (implicitly, younger persons with an ICT background). Activists are also either not aware of security and privacy risks or treat them as low priority. The critical, ongoing, issue is the problem of managing their very uncertain financial base. Hence:

Olivia: “Our biggest fear is that we will not be able to sustain this in the terms of funding”

Brad: “considering that most of our donations are from EU, political crisis that culminated in the last period could lead to canceling of *EU Instrument for Pre-Accession Assistance* IPA funds and practically that would be a *major* blow to our work…”

All participants are using external financing for ICT and infrastructure costs, and cessation of funding might, with high probability, mean not only less ICT use for conducting activities, but also probably the disappearance of activist organizations or severe weakening of their influence. Here, models such as those from Goecks et al. (2008) should be proven for applicability.

This paper has identified the main activists and their practices in recent years in RS. It also provided a structured picture of their needs and the various constraints under which they act. Although it might be said that all NPOs of this kind act under constraints, we have tried to show that they are especially acute in this situation largely because the established and regular interplay between State and civil society which usually entails stable intermediate political and legal institutions, is far from mature here. The role of social media is even more pronounced as a result since it basically becomes the only vehicle for activism other than direct action. As mentioned earlier, this paper presents the results of the first phase of a multi-year design case study.

It provides an original contribution through identification of following needs of RS and global activists under an unstable regime:

- the need for structured approach to cyber security, privacy and anonymity within activist circles and the NPO sector
- the need for specialized training (beyond basic ICT) tailored for cyber activists, the specific region and based on available means
- the need for sustainable models within ICT outsourcing and use of external freelancers within cyber activism
- the need to support practices enhancing self-learning and knowledge transfer within the specific B-H/RS setting.

Our focus is on the relationship between the emergent/fragile democratic contexts, the kinds of activism that seem to be prevalent, and how best to support them. In the near future we will implement one improvement from this section as a prototype together with activists (e.g., implementation of one security control for B-H activists following a participatory design approach similar to Caveat (McPhail et al. 1998) or Come_IN@ Palestine (Aal et al. 2014). Implementations will be made available to the activists for a test in a real-world practice ultimately leading to improvement of their communication practices. Considering the further research, case studies of particular areas make comparison with state-of-the art more valid and unfolding one of the events (e.g., park protest) would both better illustrate our research and support our vision of how ethnographic, qualitative research should be elaborated. Planned follow-up design activities will further contribute to CHI research on activist networks and provide sustainable support for activists worldwide.

4.2 Cyberactivist: Tool for Raising Awareness on Privacy and Security of Social Media Use for Activists

4.2.1 Abstract

Bosnia-Herzegovina (BH) and its entity Republika Srpska (RS) are among the most fragile democratic environments in Europe. In the first phase of our long-term participatory design case study, we engaged the some of the main activists in RS/BH, providing a structured picture of their practices in recent years, concrete needs, and the various constraints under which they act. Our research highlighted importance and utilization of the social media for the activism in the region, but also problems such as limited budgets and know-how of the activists, intensive outsourcing practices, and a lack of awareness regarding data privacy and cyber security. Due to the perspective of RS/BH, the rising number of threats and impact incidents, and activist experiences from other unstable regions, we propose a more structured approach to privacy and security within activist circles and non-profit organizations. As the initial step in the second phase of our study, we offered a prototype of the free web application “Cyberactivist” to RS/BH activists for user tests. Based on their qualitative feedback we defined the functional and non-functional requirements on further improvement of this privacy and security awareness tool. In the next phase, we will technically address their direct feedback, as well as design recommendations from relevant research and user experience literature. We also plan to propose design method improvements, design corresponding privacy and security trainings and to further internationalize the tool.

4.2.2 Introduction

Bosnia-Herzegovina (BH) and its entity Republika Srpska (RS) are among the most fragile democratic environments in Europe. The relationship between this political environment, the kinds of activism that seem to be prevalent, and how best to support them is in the focus of our research. Our research follows the methodological concept of long-term design case studies, as it was elaborated for practice-oriented design research (Rohde et al. 2017; Wulf et al. 2011; 2015). Design case studies are ethnographically informed studies that are "describing the original social practices, the design discourse, the design options considered, the appropriation process, the effectiveness of the artifacts’ functions and the emerging new social practices" (Rohde et al. 2017). They are based on a participatory and cyclic approach of analyzing social practices in a pre-study, creating, and implementing design solutions and evaluating the appropriation practices of users. This paper presents essential insights from the analytical pre-study and participatory design phase of a long-term design case study that is still ongoing.

In the first phase of our design case study, we identified the main activists in RS, providing a structured picture of their practices in recent years, concrete needs, and the various constraints under which they act (Tadic et al. 2016). Empirical investigations of social media use and qualitative interviews with the country's activists indicate their strong interest in information and communication technology (ICT). Especially social media in the region is even more relevant since it basically becomes the only vehicle for activism other than direct action. Benefits for the use of ICT and social media by activists include e.g., more efficient access to their target group, easier information sharing with the general population, and quicker reaction to spontaneous "offline" activities (cf. Tadic et al. 2016, Lynch 2017, Fullam 2017). At the same time, research highlighted problems of the activists such as limited budgets and know-how, intensive outsourcing practices, and a significant lack of awareness regarding data security. Although our activists are digitally very active and consequently ICT-literate, they are largely self-taught, being neither ICT-professionals nor "digital natives". After we conducted problem-centric interviews with six cyber activists, we clustered their needs and our observations in the following categories:

- a structured approach to cyber security, data privacy and anonymity within activist circles and the NPO sector
- specialized trainings tailored for cyber activists, the specific region and based on available resources
- support for practices enhancing self-learning and knowledge transfer within the specific RS/BH setting.
- sustainable models within ICT outsourcing and use of external freelancers within cyber activism.

Due to the perspective of RS/BH, the rising number and impact of privacy and security incidents, and an increasing relevance of social media and activist experiences from e.g., Turkey or „Arab Spring", we believe that a more structured approach to privacy and security within RS/BH activist circles and non-profit organizations is needed. Aiming to address these developments and elements 1) - 3) listed above, in the second phase of our design case study, we decided to implement a prototype of a web application named "Cyberactivist" for awareness in the areas of privacy and security. Following a participatory design approach like Caveat (McPhail et al. 2008) or Come_IN (Aal et al. 2014), we made our prototype software available to the RS/BH activists for a test in a real-world practice ultimately leading to

documentation of clearly articulated requirements for improvement of their communication practices and the tool itself.

In section two of this paper, we are looking at the related state-of-the-art work regarding the social media impact within global activism and the related privacy and security considerations. Section three provides an overview of the functionalities of the tool and section four follows with the summarized outcome of the RS/BH activist experiences during and after the test of the "Cyberactivist" prototype. Last section provides an outlook on planned next steps and research possibilities in this context.

4.2.3 Related Work

Social media based movements and their members leave behind digital footprints that authoritarian powers can exploit for the surveillance and oppression (Morozov 2011), e.g., using provocateurs and bots (Drake et al. 2016; Gritzalis et al. 2014). Gritzalis et al. (2014) looked at social media focusing on one side with insider threat prediction and prevention, connecting malevolent insiders and predisposition towards computer crime with personality trait of narcissism. At other side, regardless of national scope, an important social threat is based on user generated content exploitation and leads to political affiliation profiling. Activists are a very relevant group here, esp. within authoritarian systems and even with potential employers. According to Drake et al. (2016), human resource departments increasingly use social media screening, which produces negative reactions of the candidates in the US. If this would be the case in RS/BH, where non-employment is high and cyber activists can be marked as the opponents of the regime, they might be having additional difficulties finding jobs, if they are not careful with the information published online. Kazansky (2015) argues that many "difficulties associated with the protection of digital privacy are rooted in the framing of privacy as a predominantly individual responsibility". This is very visible regarding Terms and Conditions of social media; although users of social media platforms are poorly informed about the changes in the privacy policies, it is often "setting forth the expectation that the user has been educated enough to now make decisions in their best interest".

Social media relevance in regard to the privacy and security differs over activist heritage (Trepte & Masur 2016), age, gender (Madden 2012, Madden et al. 2013), habits (Magolis & Briggs 2016), and changes over time (Stutzman et al. 2014). Trepte & Masur (2016) conducted a comparative study on social media use with focus on privacy aspects within five nations. Although a majority of users stated that is "important to prevent risks that might arise

from privacy related behavior", they had significantly different implementations, such as anonymizing their identity or self-disclosure. Mentioned implementations might easily be customized to address the needs of activists of other nations. Study participants reported that they had not yet experienced many privacy violations. In our case, RS activists have also their specific attitude, similar to the part of the attitudes from Trepte & Masur (2016) which must be considered within the tools supporting their engagement. With effectiveness and practicality in mind, we implemented a prototype of a web application „Cyberactivist" for awareness in the areas of privacy and security of social media, described in detail in the next section. It also might be used in other geographic contexts, similar to implementations of Trepte & Masur (2016). Madden (2012) has shown how different population structures have a different understanding of privacy, its enforcement and importance in the social media context. This may very well apply to our activists. Magolis & Briggs (2016) focused on undergraduate students' experiences with social network system privacy. Students worried about their privacy being violated by someone physically locating them still felt comfortable sharing their personal information. More media literacy leads to better awareness about risks of sharing information on social media. This supports the thesis on need for specialized training for activists identified by Tadic et al. (2013). Stutzman et al. (2014) compared Facebook users to understand how their privacy and disclosure behavior changed between 2005 - 2011. Besides concluding that users exhibited volatile privacy-seeking behavior, from less disclosure in the first years to an increase towards the end of the study, they warned from the often non-transparent "silent listeners". Due to the increase in amount and scope of personal information that users revealed privately to other connected profiles, more information is available to Facebook itself, third-party apps, and indirectly advertisers. Authors of this paper assume that these findings are becoming even more relevant for numerous cyber activists, if we extend the list of "silent listeners" to state-related apparatus and highlight low privacy awareness of the activists present on Facebook (e.g., low interest in terms and conditions).

Following a participatory design approach (cf. Aal et al. 2014, McPhail et al. 1998), our implementation was tested by the activists in their real-world practice. This led to the tuning of our tool based on direct interaction, and ultimately improved activist communication practices. We also orientated us on insights of e.g., (Kar & Ghose 2014; Petkos & Papadopoulos 2015) and recommendations from best practices such as Deutschland Sicher im Netz (2017). Petkos & Papadopoulos (2015) proposed a framework including an open-source implementation with semantic, hierarchical scoring structure for raising the awareness of

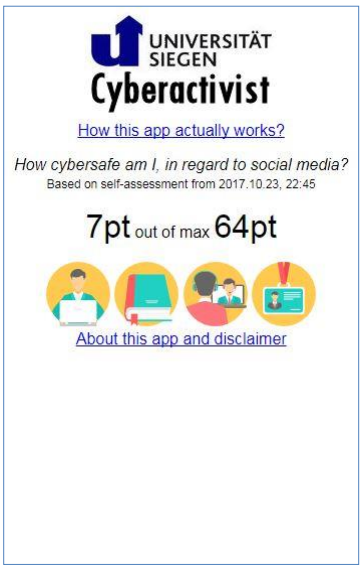
social media users with respect to the information that is disclosed and that can be inferred by third parties with access to their data. It enables users to browse over different privacy-related aspects considering both information that is explicitly mentioned in users' shared content, as well as implicit information, that may be inferred from it. Kar & Ghose (2014) also claims that ICT and social media enabled better access to personal and location information of another person, and activists may not be aware of the possibilities here. Despite having regulatory policies, it is possible to extract quite exact location information of a person over time by using volunteered or contributed geographic information available from social media sites (e.g., GeoAPI of Twitter).

Although privacy and security requirements are sometimes in conflict, we can reasonably raise both aspects using tailored approaches (Wang et al. 2013, Saad & Khan 2016) and by creating visibility over vulnerabilities of an activist or his environment (Singh et al. 2015). It is also important to consider differentiation of the social groups in their attitude towards privacy and security when developing ICT solutions (Kazansky 2015) and unconventional approaches to promote privacy and security such as using celebrity engagement in social media (Tsaliki 2016). Taking the example of one group of human rights activists, Kazansky (2015) highlights the importance of developing a collective approach to address their digital privacy and security needs. Digital security strategies cannot remove all threats; they can only mitigate their effects and deal with numerous elements such as authentication on Facebook. We included the question about the Facebook authentication into the Self-assessment within our prototype (see next section of this paper). Singh et al. (2015) introduced methods for determining the amount of information that can be ascertained using only publicly accessible data and provides a framework for determining a user’s web footprint. Threat of user’s attributes that may be inferred by an adversary using only public sources of information has been reconfirmed by analysis across multiple social networks. The same method can be applied by cyber activists and other individuals to assess and act upon their own exposure in the public media.

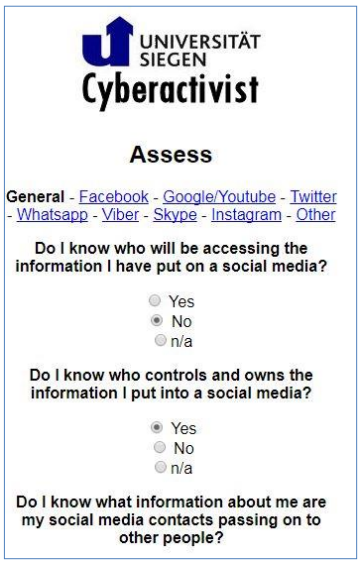
4.2.4 Web Application “Cyberactivist”

The development of the initial version of our web application “Cyberactivist” (in English and Serbo-Croatian language) took six months in 2016, using HTML, JavaScript and CSS. One of the paper authors has written the whole source code of the initial version of the prototype that was provided to the activists for the test.

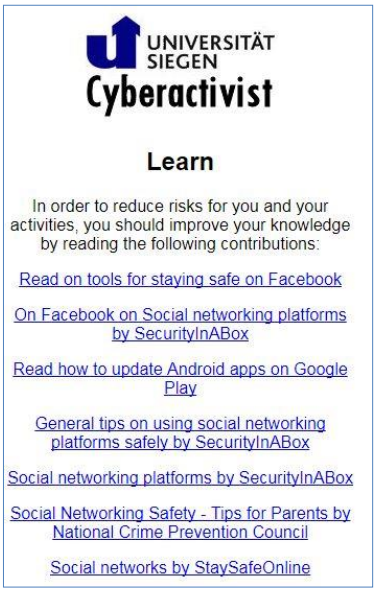
Primary functions of the tool are to enable self-assessment of privacy and security in the context of social media and make results transparent to the user, then dynamically point to open, external, self-learning resources esp. in areas marked as “blind spots” and volunteering opportunities. “Cyberactivist” consists of four sections, which are represented by the icons on the primary screen after the application start: Self-assessment, Self-learning, Contribute, and My Profile. In addition, there is information about the so called Cyber safe score of the self-assessment, visible only after the performed self-assessment, and hyperlinks to two information pages: About the application and How does this application work.



6: Main Screen Showing Sections and Cyber Safe Score



7: Self-Assessment Section / Questionnaire



8: Self-Learning Section / Recommended Reading

9: My Profile Section

Self-assessment (Fig. 7) and My Profile (Fig. 9) sections enable users to gain transparency about the risks within their social media environment and to see how they are positioned regarding these risks. We are using easily understandable, user-centric language, knowing the average ICT proficiency of the target group, to help them gain insight and derive appropriate action. Section Self-assessment contains nine groups of questions: 25 general questions, applicable to most social media platforms, then specific platform questions on Facebook (11 questions), Google/Youtube (8), Twitter (6), WhatsApp (4), Viber (4), Skype (4), Instagram (6) and one group reserved for other platforms such as LinkedIn (3), which can be answered through multiple-choice text options (e.g., "yes", "no" and "I do not know"). An example of a question is "Do I know who will be accessing information I have put on social media?". The question groups are focusing on the most frequently mentioned ICT tools and social media platforms mentioned by the activists by Tadic et al. (2013) and publicly available ranking information (cf. Kallas 2018). When results are saved, they are being recorded on the activist's device using the local storage functionality of HTML and not transmitted to any remote server. The selection of questions and their formulation have been based on experience of one of the authors of this paper, as well as on similar international questionnaires and assessments such as (cf. Deutschland Sicher im Netz 2017, Sicherheitscheck 2017, Internet Privacy Practices 2017, Online Privacy and Security Questionnaire 2017, USAID Privacy Office 2017, Academic Frontier Project 2017, Purdue University 2017, Warwick University 2017, Federal Trade Commission 2017, Kumaraguru 2017). The Section My Profile shows the data about the user available within browser he uses, e.g., whether Java is activated or what is the geographic location. It also enables the user to set the language of the application.

The main screen shows a so called "Cyber safe score" (Fig. 6). This score is calculated based on the number of positive ("plus" point) and negative answers ("minus" point) from the self-assessment with the maximum score of 64 points being achievable. An example of the positive/negative answer is "I have/have not latest version of Twitter installed on my devices". On the main application screen, the user is also being given an instruction to perform a self-assessment before being able to use the application's full functionality and find out "how the tool actually works".

Section Self-learning (Fig. 8) offers a customized array of reading materials based on the Cyber safe score and improvement areas. Most materials are articles published by the relevant social media platforms, non-profit organizations, or media with direct actionable advice on

improving security, privacy, and anonymity. In the case of the mentioned Twitter answer example, it would be a reading material related to “software patching” or “privacy and security settings of Twitter”. It supports preferred way of (self-)learning of the RS/BH cyber activists, caused by resource limitations (e.g., training budget). Every click in this section opens an additional web browser window and shows the original web page outside the “Cyberactivist” application.

The Contribute section aims at knowledge sharing and multiplication effects, providing a non-customized list of organizations and websites providing privacy and security advice to activists, e.g., TacticalTech (2018). The list is based on the selection of the authors, based on the background of RS/BH activists.

“Cyberactivist” does not collect, process, or send any information about the users or their online behavior to the author or any other subject. The application does not use cookies. All links included in the Self-learning section are to third party websites, which have separate privacy policies and the authors therefore have no responsibility or liability for their content or activities.

The format of the application - web-based, platform independent, free - is also chosen based on the activists’ usage of phones and PCs as primary hardware. Making the “Cyberactivist” source code open, with no modification and expansion constraints, improves its reach among activists. After completion, the authors, and their academic institution plan to publish and keep the software free and open source providing a clear value adding to the activist and developer community.

4.2.5 Participatory Design: Feedback and Possible Improvements

After the development of the application, we have shared a link to the prototype for the test with the selected activists. We contacted all the activists who participated in our former research (cf. Tadic et al. 2016) and additional new activists we identified monitoring social media activities in the RS/BH.

Five activists responded to our invitation (Table IV). We asked them to test the application and did not provide them with any information besides that the web application is focused on privacy and security. They tested the application on one day but did not invest longer than an hour of their time. Neither usage data nor self-assessment results were transmitted to the paper authors during or after the test. Activists also committed to the interview in the Serbo-Croatian language after the test, to document their impressions and feedback on possible tool

improvements. The activists provided us with almost four hours of responses which were digitally audio-recorded in five separate sessions between May and September of 2017. One activist complemented his audio statement with an e-mail response. Skype with an audio recording plug-in was used as an interview tool. The key findings of our interviews were transcribed in English language and comprise approximately 50 pages.

All activists suggested that the application is simple. They all also agree that the purpose, background methodology, and the user interface of the "Cyberactivist" application has to be further sharpened. There is a need to further optimize the main screen. Brad posed a question: "Is the tool meant for single use or for reuse?". Kevin did not even open sections *Self-learning, Contribute, and My profile* as access to these sections was not visible or intuitively displayed. With regard to navigation within the app, Alena suggested that a "Go Back" key is missing.

IV: Interviewed Activists / Participatory Design Phase

Pseudonym	Birth Year	Role / Active since	Participated in our earlier research
Brad	1980	Project Manager at local NPO, 2006	Yes
Ela	1984	Project Manager at the local branch of an international NPO, 2008	Yes
Adam	1981	Member of international NPO focused on the RS, 2008, located in Austria	No
Kevin	1981	Local journalist / an individual activist	No
Alena	1980	Individual activist for disabled population	No

Adam suggested establishing separate scores for security and for privacy; as referenced in section 2 of this paper, security and privacy aspects are not always correlated. The methodology to calculate the *Cyber safe score* raised many questions among activists. Originally planned as the simple, high-level information of displaying general protection status, *Cyber safe score* did not fulfill its purpose. The score was unclear for most activists (e.g., Ela: "I got 35 out of 65 points…" - what does it concretely mean, where are my weaknesses, what do I need to improve). The outcome from the self-assessment should be visible immediately, and not only later through links in the section *Self-learning*. The outcome should be explained in more descriptive language, rather than only by a number. Adam considers himself experienced within security and got only 2 points after the self-

assessment. The other activist did not understand the logic of adding “plus” and “minus” points.

Most activists tested the tool on the laptop or desktop computer, not on the mobile device. However, Adam suggested that our application should be further customized based on the platform used (e.g., screen resolution, native user interface). The platform should also influence the offered advice in the *Self-learning* section. Differentiation between PCs and mobile devices in the answers within the *Self-assessment* section are also proposed, as usage patterns are differing.

Regarding the *Self-assessment* section, Adam commented that 25 questions in the general part of this section might be too much and proposed separation over several screens/pages. Another idea would be to show the progress of the questionnaire (“how much I still have to go?”). Almost all activists felt that there are lots of repetitions of the similar questions (e.g., same formulation “did you perform an update for… Twitter, Facebook, Whatsapp…”), however they meant that the “questions are clear”. Several questions in this section contain formulation “Do I or my organization use…”; Kevin suggested to clearly separate the two, as the answer may differ. Kevin’s proposal was also to add the answer option “I don’t care/It’s not important” to existing possible answers “yes/no/don’t know” in the self-questionnaire. Kevin also suggested reconsidering which questions are suitable for the “general questions” category. For him the question “do I trust my connections” would be differently answered for different social media platforms, e.g., for Facebook and Twitter. Two or more predefined answers are offered for every question in the *Self-assessment* section based on the multiple-choice logic. Alena claimed that there is no need for any choice to be marked as default, as it is with the choice “I don’t know” in our case. Activists also suggested adding or rephrasing some questions such as “how to add to the group on social media, limiting member’s access” or „would your identity disclosure jeopardize your close people/relatives”. They claim that is positive that a person is not asked on all tools if they do not own an account on this specific social media.

The first improvement proposal for the *Self-learning* section was that the introduction text should not be shown if the self-assessment is not done. Some of the activists such as Adam did not notice the correlation between the *Self-assessment* and *Self-learning* sections. Activists also claimed that the explanation of the results is needed, such as “…because you don’t understand X, you need to read Y and Z”. Therefore, a clear link needs to be established between “negative” answers from *the Self-assessment* section, “minus” points of the Cyber

safe score and the proposed reading materials in the *Self-learning* section. Optimally, related reading materials should be grouped. Authored privacy and security advice is welcome, according to Ela.

Looking at the *Contribution* section, Adam asked whether the listed organizations want/need help or volunteers at all. The others found this section useful as it is. As RS/BH NPOs and activists are struggling with resources (Tadic et al. 2016), Brad suggested an additional feature „find/engage an expert" (e.g., specialist for IT security or video production). He also proposed to integrate some "advertisement" in the tool such as „you are an IT expert - do you want to help and engage in our activities?".

The information in the section *My profile* was found to be useful, however not always self-explanatory (e.g., web browser information as "user agent string").

Brad suggested the replacement of the term "activist" with „socially responsible person", due to "negative connotation" of the term. In general, activists asked that tool's goals, benefits and "flow" are described more clearly in the tool itself (e.g., are results of self-assessment sent somewhere for analysis, how is the score calculated). In addition, better instructions on the tool proper usage are welcome.

In addition, all activists suggested that the used text for a Serbo-Croatian version can be improved. Activists advised the use of fewer Anglicisms in the text and less synonyms esp. in technical context (e.g., "data privacy" vs "data protection"). They also made proposals on how to increase readability, through consistent use of the local alphabet (e.g., "č vs c"), adequate font size and text margins on the different platforms. The *Self-learning* section was referred by Ela as useful as it's good to point to sources and practices from other countries. Other activists were only partially satisfied with the fact that all reading materials offered by the tool as a result of the self-assessment are in English (and not in Serbo-Croatian). This feedback is a good reminder that text quality and thorough localization of the tool plays an important role for acceptance among the activists.

This very qualitative feedback from the activists gathered specific functional and non-functional software requirements and enabled multiple ways of improving the tool. Several ideas for tool improvements are coming from state-of-the art research, e.g., aligning it to models such as "privacy nudge" (Wang et al. 2013; Saad & Khan 2016), considering integration with approaches such as "FaceCloak" (Luo et al. 2009) or adding features such as "celebrity cause" Tsaliki (2016), which might be considered in future work and tool

adaptations. Research on behavioral decisions and soft paternalism to design mechanisms led to development of so-called “privacy nudge” for Facebook users (Wang et al. 2013). This alarm reminds Facebook users to consider the content and context of the information before posting them, helping individuals avoid regrettable online disclosures. Nudges provide visual cues about the audience for a post, time delays before a post is published and gives users feedback about their posts. Adaptation of this nudging might prevent activists’ unintended disclosure. Saad & Khan (2016) also argue the idea of nudging the user with “Privacy Nudge” to help people make better privacy choices and decisions on online social networks. The proposed model will nudge users while posting by calculating Privacy Score and accessing last modified privacy settings for users which will alert users to adjust their privacy settings. FaceCloak protects user privacy on a social media by shielding a user's personal information while maintaining usability of the site's services (Luo et al. 2009). This Firefox browser extension for the Facebook provides fake information to the social media and by storing sensitive information in encrypted form on a separate server. Although oriented on one platform only, it is an interesting concept that could be a measure related to our “*Cyber safe score*”. Celebrities, such as movie actors, often take up an active interest in the “good causes” such as prevention of engagement of children as soldiers in Africa. Their posts on the cause in the social media help draw attention to the cause among their numerous followers. This might be an opportunity for cyber activists, also in the context of awareness for protection of their privacy and security and lobbying for e.g., less surveillance in authoritative societies (Tsaliki 2016)

The authors themselves also identified ideas on improving the tool, such as those improving user experience, building a more intuitive graphical user interface, and adding relevant information sources.

4.2.6 Outlook

Especially the more detailed evaluation of users' appropriation of our prototype in the practice goes beyond the scope of this paper and will be object of future research. We base our original contribution to the HCI knowledge corpus on the long-term design case study which enabled numerous insights into practices of political activists in RS/BH, which led to a tool “Cyberactivist”. Our presentation includes the relevant state-of-the-art research, online and offline experiences with our prototype, unfiltered feedback of the activists, and differentiation through simple, yet unique awareness and self-learning capabilities on social media.

The tool enables activists to understand, address and mitigate the privacy and security risks related to use of social media. The authors plan first to adapt the tool based on the input from the section four of this paper, and eventually to publish it cost-free in multiple languages making it available to the global activist community. This will follow an intense exchange with other HCI researchers which have worked in multiple other geopolitical regions (e.g., Middle East) and incorporation of their thoughts on applicability and target group reach. In addition, in further publications we plan to continue our design case study by observing the development of the ICT and esp. social media use in RS/BH.

Authors and the research community can further refine the underlying research method, e.g., regarding the precision of the questions asked in the interview phase, or evaluation and consolidation of sometimes opposing improvement proposals of the activists. Industry best practices such as Scrum within agile software development (cf. Schwaber & Beedle 2002) are a great opportunity for improvement of both, our method and quality of the tool. Continuous presence of the activists in the role of the "customers" during the development "sprints" would directly increase the quality of the tool, and potentially fully remove the need for interviews after the implementation of the new tool functionalities.

Our strong belief is that the tool's impact would be raised if activists would receive free tailored and localized training on privacy and security aspects. In the future, authors will work on the conceptualization of such trainings and/or information campaigns. We believe that this holistic and integrated socio-technical approach will serve as an open, extendable, scientifically founded and practically easily applicable awareness instrument for activists in fragile democratic contexts worldwide.

4.3 Security and Privacy Aspects of ICT and Social Media Use by Activists in Post-Conflictual Societies

4.3.1 Abstract

Socio-political activists in both Republika Srpska (RS), an entity of Bosnia-Herzegovina (BH) and in the Middle East and North Africa (MENA) region use ICT and social media extensively to promote and support their activities. However, they are exposed, often unaware of the risks and risk remediation measures related to social media use. In this paper, we compare data from our long-term case study in RS/BH with research from the MENA region in order to identify similarities and differences in threats experiences and resources on offer. This paper specifically highlights the challenges activists from both geographies face regarding ICT and social media use and, using the combination of qualitative content analysis, field/empirical studies and abduction based on grounded theory, derives a four-layer, "pyramidal" threat model. The model describes defamation, legal action, material loss and physical harm, and is meant to sensitize activists to the range of threats they might be subject to in the context of security and privacy. Based on this model, we further enhance and complement our technical design, Cyberactivist, to raise awareness and enable risk remediation, not only in RS/BH and MENA, but also in a global context.

4.3.2 Introduction

Bosnia-Herzegovina (BH) and its entity Republika Srpska (RS), covering 49% of its territory, are one of the most fragile democracies in (southeastern) Europe. It constitutes a post-conflict, transitional environment with low GDP, poor ICT infrastructure and a complex landscape of "lively" socio-political activism (EU Commission 2019). Such a situation is, we argue, in many ways comparable to those of the Middle East and North African (MENA) region (esp. Israel/Palestine, Iraq, Iran, Tunisia or Syria), albeit with a different balance of threats. Since 2012, we have conducted an ethnographically informed design case study of RS/BH with the focus on the ICT and social media use practices of socio-political activists (Tadic et al. 2016, 2018). In parallel, there are numerous CHI/CSCW studies of the MENA region, such as those by Wulf et al. (2013a,b), Rohde et al. (2013) and others. The empirical and ethnographic research of the ICT and social media use of both geographies, we argue, have implications for other regions of the world where similar conditions apply.

In the context of privacy, security, and anonymity, (Tadic et al., occasional paper 2019) identified three major issues in RS/BH regarding social media and ICT in general: ignorance, exposure and "no remedy". Most of the RS/BH activists are not (sufficiently) aware of

possible threats and risks, and sometimes even explicitly choose to ignore them. RS/BH activists are also unclear about the level of exposure of them and their families, friends and associates on social media. Regardless of the role of ignorance and overall lack of clarity about security issues, RS/BH activists have limited means to protect themselves and their stakeholders, making the remediation of even known issues not always possible. There is an evolving landscape of threats related to security and privacy of ICT and social media use which is not limited to RS/BH, but very relevant for other (post-)conflictual, fragile societies such as those in the MENA region as well. Here, we identify the threats faced in relation to ignorance, exposure and lack of remedy and then apply a design case study approach generate a model of the threat hierarchy. The technical design, Cyberactivist, described by Tadic et al. (2018), focusing on the security and privacy awareness aspects, was designed, prototyped and discussed with the RS/BH activists and international CHI/CSCW researchers in previous years. In this paper, we engage in comparative work, based on the experiences from the MENA region, with a view to establishing whether our model, and the technology, could contribute a more general application. Therefore, three research questions for our paper are:

- is RS/BH comparable to the MENA region regarding ICT and social media use by activists?
- can threats resulting from this use in the context of security and privacy be generalized and structured?
- can the tool Cyberactivist be adapted for the MENA region, and combined with other tools to ensure a holistic response to these threats?

We hope that the paper build on existing research on the Western world's position towards privacy and security of social media, can contribute to an understanding of what difference there might be in privacy and security related attitudes between stable, developed, truly democratic societies and in those which are fragile, developing, and transitional.

In section 4.3.3, we look at the state of the art. Section 4.3.4 briefly summarizes the applied methods. Section 4.3.5 then focuses on the similarities of the RS/BH and MENA regions, while section 4.3.6 provides a perspective on various security and privacy threat types in the context of ICT and social media use. Section 4.3.7 deals with the possible adaptation of the related technical design and tool, Cyberactivist, while the section 4.3.8. summarizes conclusions and provides an outlook on future work.

4.3.3 Related Work

There are numerous studies of use of ICT in political activism in the MENA region. Howard et al. (2011) and Tufekci and Wilson (2014) investigated social media, esp. Facebook and Twitter use in Egypt during and after the Arab Spring. Tufekci and Wilson (2014) noted that MENA events "are now being shaped by a new system of political communication which sets into sharp relief the importance of digitally mediated interpersonal communication". Rohde et al (2003) investigated ICT use within the NGO sector of Iran and then again in 2013, focusing on activist interaction and trust building. Also, Zhou et al. (2010) quantitatively analyzed Twitter usage and information propagation dynamics during the post-election protests in Iran in 2010. Wulf et al. (2013a) were "on the ground" in Palestine, looking at the protesters and their social media use for facilitating protests against the wall in the West Bank. Research on the use of ICT and social media in Israel and Palestine was in the scope of Tawil-Souri (2012), Kuntsman and Stein (2015) and Boulus and Bjorn (2019). The starting point for the Arab spring, Sidi Bouzid in Tunisia was visited by the Wulf et al. (2013b), where they investigated the political uses of social media on-the-ground. In 2012 and 2017 respectively, Trombetta and Wulf et al. dealt with Syria, which faced brutal civil war, noting the way in which traditional, new media and mobile media use intersected in the conflict zones. Maitland et al. (2015) described youth mobile phone and Internet use in the Jordananian Za'atari refugee camps for Syrians, noticing that social media use doubled in intensity in the refugee camp compared to the intensity of use by Syrians in Syria. Interesting observations of "Twittersphere" by Freelon et al. (2015) include high fragmentation among pro- and anti-Assad communities and the fact that even anti-Assad communities were differentiated among national and ethnic lines, with e.g., Kuwaitis and Saudis who "had largely similar approaches to Syria but tended to interact with their co-nationals more intensely than with a pan-Arab community". Freelon et al. (2015) remind esp. international CHI researchers not to look at the MENA as homogeneous off- or online identity or community. Klausen (2015) looked at social media, esp. Youtube and Twitter and their use by Western foreign fighters in Syria and Iraq, concluding that social media is used by the jihadists "for purposes of recruitment and indoctrination, as well as to build a transnational community of violent extremism" (p. 17). Mark and Semaan (2008), in their study of Israel and Iraq, described how ICT "played a major role in providing people with alternative resources to reconstruct, modify, and develop new routines, or patterns of action, for work and socializing" (p. 137). They describe both the "highly-technical society" of Israel and the technologically "limited and controlled" Iraq but claim clear commonalities through "increased situational awareness of others in their social

network" in times of disruption (p. 145). Langer et al. (2019) researching counterterrorism narratives, found that "success stories, determent, self-promotion, linguistic differences, localizations, visualization and suggestions are characteristics of social media posts that promoted most reactions by the target group" (p. 753) and proposes the use of "anti-narratives" related to terrorist narratives and "integration with other counterterrorism efforts". Gyöngy (2019) also looked at the aftermath of new media use in the Syrian conflict, and on a similar note, again in the (post)-conflictual regions, De Castro et al. (2019) write about ICT use in conflicts in Colombia. In all the above cases, researchers documented social practices related to the use of existing ICT artefacts and produced and/or introduced new ICT artefacts. An understanding of security and privacy aspects may improve both the usage of ICT artefacts in the region, as well as ICT artefacts themselves.

In many countries outside of the "Western world", information integrity and individual privacy is not protected by the law, or is even, on the contrary, regularly jeopardized by state actors. Bradshaw and Howard (2017) conclude that "organized social media manipulation occurs in many countries around the world" (p. 22). They add that "individual social media users can spread hate speech, troll other users, or set up automated political communication campaigns" but also "major governments and political parties dedicating significant resources towards the use of social media for public opinion manipulation" while the "cyber troops have multiple affiliations, funders, or clients" (p.22). Mosco (2019) also claims that search rankings and newsfeeds "are filled with material that bears little relationship to accuracy and truth, including racist, sexist, and other extremist content" and adds that EU GDPR "offers a good beginning". He then adds that is "essential to return control over data and information to those who provide it – including individuals who make use of social media sites, and organizations that create the research and the stories vital to the preservation of democracy" with users being able to "withdraw information from social media sites and provide it to those of their choosing". Mosco (2019) also proposes that "strict rules governing the uses and abuses of algorithms – such as those that filter searches through commercial imperatives – must be enacted, with a special focus on making them as transparent as possible". Although the literature about privacy and security aspects of ICT and social media use is not as extensive as in the Western world, looking at the MENA and Eastern Europe situation around privacy and security, we found some suggestions. Speaking about Kuwaiti people's attitude towards privacy in the commercial domain, the majority "felt safe while entering their personal information" but "a significant decrease in trust was noticed when asked whether the site seemed to be capable of keeping customer's data safe" (Shama and AlMeraj 2019, p. 48).

Ahmed et al. (2017a) point out that “enactment of a surveillance law carries the risk of suppressing individuals’ voices and may eventually destroy the democratic environment in a country”, claiming that an “individual’s right to privacy is inevitably associated with the democratic development of a country” (p. 913). Pearce and Kandzior (2012) found that the Azerbaijan government has “successfully dissuaded frequent Internet users from supporting protest and average Internet users from using social media for political purposes” (p.283). Vaziripour et al. (2018) claim that for most Iranians living inside of the country, “privacy is important, yet only about 10% use end-to-end encrypted chat at least sometimes” (p. 10). Many of those who send sensitive information report trusting Telegram, one of the most secure IM/social media tools, but do not use e.g., initial authentication “handshake” or misplace trust in the context of the app’s channels. One half are “sending sensitive information while using the application, indicating that Telegram is not meeting their expressed privacy preferences”. Shklovski and Wulf (2018) claim that activists relying more on mobile devices and telephony need to be aware who owns and controls that infrastructure and how vulnerable the infrastructure is to modern military surveillance technologies. The authors of that paper argue “users of social media and communication technologies have a right to an understanding of surveillance practices by the state, the platforms and the military industrial complex” (p. 396).

We believe that the intersection point of ICT and social media use in (post-)conflictual societies and the situation concerning privacy and security of activists and their environment is one where both a clear academic and practical contribution can be made. This has explicitly been called for by numerous CHI/CSCW researchers, such as Tufekci and Wilson (2014), claiming that “the conditions under which citizens overcome the potential risks of online activism in repressive regimes are of obvious importance for future researchers” (p. 377).

4.3.4 Method

This paper presents the results of the last phase of a long-term design case study, aiming to improve the secure communication practices of socio-political activists. Design case studies follow a long-term participatory and iterative approach: analyzing social and usage practices, designing a solution, implementing, or improving solution prototype, and observing and evaluating the usage practices of users, which may lead to change in socio-political practices (cf. Rohde et al. 2017 and Wulf et al. 2011). Since 2012, the authors have investigated the use of ICT and especially social media by civil society organizations and political activists in RS/BH. Our project relies primarily on qualitative, explorative methods (observations,

interviews, workshops), web space and social media content analysis, partially integrating ethnographic methods (like participant observations). The method around RS/BH research is described in detail by Tadic et al. (2016 and 2018). In the first phase of the design study, we identified the main RS/BH activities of activists, especially their use of traditional channels and of social media and tried to fully understand the context of their ICT use and their needs in respect of privacy. In the second phase, we have built a technical design Cyberactivist satisfying some central RS/BH activists' needs. We tested the prototype first with RS/BH activists, and then with non-RS/BH activists and CSCW/CHI researchers. Following this, the prototype was iterated, based on the feedback and further research findings about issues related to security and privacy of social media use Tadic et al. (occasional paper 2019). The last, current phase contains periodic identification of changes in RS/BH and the global activist context (in the case of this paper in the MENA region) regarding ICT use and needs. The goal is to both "globalize" and "localize" the tool. That is, to make it relevant for use in a number of contexts. We aim to make a final, open version of Cyberactivist (and optionally, the context/tool training) available to the activist community in RS/BH, the MENA region and to all other interested activists.

This paper builds on the assumption that there are similarities between the RS/BH and the MENA region in the context of activism, and that the threats around security and privacy in the context of social media and ICT can be structured. Based on that, our existing technical design, Cyberactivist, can be enhanced to serve not only RS/BH, but diverse activists on an international scale. For comparison, we applied the principles of abductive analysis, a qualitative data analysis approach grounded in pragmatism aimed at theory construction. According to Reichertz (2009), and Tavory and Timmermans (2014), abduction "depends on iterative processes of working with empirical materials in relationship with a broad and diverse social science theoretical literature" with the goal of producing "theoretical hunches for unexpected research findings and then developing these emergent theories with a systematic analysis of variation across a study". Through our content analysis of papers relating to ICT and social media use by political activists in MENA we determined commonalities in the context of possible threats relating to security and privacy. Following this, we systematically examined the variations of the threats to be found in the accumulated data and iteratively adapted our threat model in the light of similarities and differences. We began with a thorough analysis of publications about the Middle East and North Africa, but also a couple of other geographies with conflictual and post-conflictual societies (e.g., Ukraine, Colombia). In some cases, the authors spoke with the experts/authors responsible for

MENA publications and, to an important extent, they have been personally active in both RS/BH and the MENA region. We then qualitatively analyzed popular social media posts (esp. Facebook, Twitter, Instagram) and conventional media reports related to the MENA region. In the second step, findings from similar analyses in RS/BH and the statements of eleven RS/BH activists and one Lebanese activist: Brad, John, Olivia, Anna, Grace, Ela, Adam, Kevin, Alena, Peter, Lepa and Ali (anonymized) were compared to the statements of nine CHI/CSCW published researchers Stavros, Haras, Daner, Omit, La, Siega, Cloude, Trademark and Soiram and numerous activists of the MENA region: e.g., Mahmoud and Hasan in the West Bank, X, Y, Z of the FSA in Syria, activists from Tunisia etc. (details of individual papers are mentioned in section two). Elements which were found in both geographical areas were recorded, then clustered and prioritized based on the frequency of the issues mentioned. We then identified patterns in the threats being faced by the activists, based on their interview statements, traditional media reports, and social media observations, as well as interview ratings, group discussion among experts and data analyses. This led to the comparison of the ICT use practices described in the next section and the "pyramidal" format of ex-post facto categories concerning four abstract threat/risk levels, ranked by the estimated severity of the personal/group impact deriving from low levels of security and privacy in social media. This is described in the fifth section. In total, we produced several hundred minutes of recorded material, and over 150 pages of notes and links from the content analysis, written responses (e.g., e-mails) and transcripts from the interviews with both RS/BH activists and CSCW/CHI researchers, complemented with 40 pages of notes from various MENA region papers.

4.3.5 ICT and Social Media Use by RS/BH and MENA Activists

Most CHI/CSCW community research relating to the MENA region focuses broadly on ICT use and rather less on security/privacy in the social media and activist spaces. Attention turned towards the latter issue as a result of cases around last US presidential elections, or in relation to the general handling and use of Facebook data. Nevertheless, we found elements to do with ICT and social media use that helped us to understand the environment and later the structure of the threats coming from low privacy and security.

Two major activism events in RS/BH in the last decade were the „Save the Park" and „Justice for David" protests with tens of thousands of participants online and offline over the period of several months, described in Tadic et al. (2016 and 2018). Similar protests, with an extensive combination of ICT, social media and offline activities using a variety of material and digital

artefacts were described in Tunisia's Sidi Bouzid anti-government protests and Palestine West Bank protests against the wall, by Wulf et al. (2013b,a), and indirectly in Iran, Egypt and Syria by Rohde et al. (2013), Howard et al. (2011) and Wulf et al. (2017) respectively. Most of the described events follow the model of Sandoval-Almazan and Ramon (2014), describing the stages of the protests supported by social media. Even the way that offline protests converged with social media usage was similar (e.g., choosing the site for the protests and driving the online campaign around it, Figures 1. and 2.)

10: Sidi Bouzid in Front of the Governor's Palace, Place of the Part of the Protests, and the Tents at the Site of Bouazizi's Self-Immolation in 2012 (Volker Wulf 2012)

11: Banja Luka at the "Krajina" Square, Close to RS/BH Presidential Palace, Place of the Initial Protests and the Tent of David's Father During Protests in 2018 (Ana Radinkovic 2018)

From the state-of-the-art it is apparent that "injustice" and corruption were the original triggers for the majority of protests and activism on social media both in the RS/BH, as well as in many MENA countries. Mohamed Bouazizi self-immolated in 2011 after the (unjust) confiscation of his wares by a municipal official and her aides, who had previously tried to racketeer him. His self-immolation started the "Arab Spring" (Wulf et al. 2013b). Also, in Egypt's Tahrir square protests, as noted by Howard et al. (2011), a "community of likeminded individuals, underemployed, educated, eager for change but not committed to religious fervor or a specific political ideology" became active (p. 15). In the Syrian city of Daraa in 2011,

abolition of some law and pervasive government corruption were the protest triggers, which ultimately led to a military deployment in the city and the start of the war in the country (Wulf et al. 2017). Pursuit of justice was originally in the primary interest of David's friends and father who did not accept the official explanation of his son's death in the major RS city of Banja Luka in 2018 (Tadic et al., occasional paper 2019). Similarly, traditional media (e.g., TV, newspapers) and the coverage of the protests was/is mostly controlled by the authorities in both regions, which mobilized activists towards the use of new and social media.

Activists in MENA share similar motives for the (increased) use of social media as the RS/BH activists and see it as "a crucial means by which access to citizens and other activists is made available" (Tadic et al. 2016, p. 3373). In Egyptian context, Howard et al. (2011) describes social media and esp. Facebook as a "political tool because people found it useful for amassing content and building links to like-minded individuals" (p. 7). Many activists also consider it safer (one of the Syrian protesters claimed that "Telephone networks were strongly surveilled in Assad's Syria" (Wulf et al. 2017, p. 12)). Egyptian protesters found solidarity "through social media, and then used their mobile phones to call their social networks into the street" (Howard et al. 2011). Mark and Semaan (2008) wrote that, after the war in Iraq, people "adopted new patterns in their social lives that incorporated email, IM, social networking sites, and chat rooms to socialize" (p. 134). After the war, Iraqis discussed their "opinions online on the current Iraqi situation", with "division between people supporting Saddam and those not supporting him" (p. 145) and for the first time addressed such topics such as women's rights. We also observe fairly similar usage patterns around ICT and social media in RS/BH and MENA: e-mail, mailing lists, social media, and instant messaging. Facebook (with Messenger included) is the primary social media tool for activists in all mentioned countries. While Viber and Skype dominate in RS/BH, in MENA you notice primarily SMS/texting, Twitter, and Telegram used by the activists and the opposition. Even the authorities can make extensive use of social media. Thus, Merhul of the Financial Times described how the Turkish president, during the coup attempt in 2016, identified a "rogue military group communicating through WhatsApp" and then used "FaceTime to reach a television presenter" to address the nation. For Gyöngy (2019), in the Syrian conflict, "because of war conditions and limited access to online media, the importance of professional media activists has grown" (p. 46). She also notices, "transnational cooperation not only between activists working within Syria and regional or international traditional media, but also between media activists operating inside and outside Syria". This is something Tadic et al. (occasional paper 2019) observed in the case of „Justice for David" group, where activists

and traditional media from the diaspora and from Western countries leveraged their resources to support local initiatives and gain wider (also social) media attention.

RS/BH and almost all MENA countries have circumscribed what is legal in respect of activism on social media, with various consequences for the activists (cf. Wulf et al. 2013a, 2013b, 2015). Where the RS/BH and most of MENA countries differ from Israel, are the cyber policing/defense capacities and ability to enforce these laws, where the latter is significantly better equipped, with knowledge, approach, and the resources. Glas Srpske wrote about the report on the realization of the action plan for implementation of the strategy for the fight against organized crime in 2018, security agencies of BH saw the primary challenge as a lack of capability for lawful "interception of communications such as Skype, Viber, Messenger etc." which are not possible with the existing interception software. MENA countries and RS/BH also differ in the context of the social media ban, where Iran, Syria, Tunisia, and many other MENA countries ban platforms such as Facebook, Twitter and popular instant messaging platforms, whereas RS/BH does not have such bans. RS/BH and MENA countries have different surveillance and cyber capabilities. We discuss this aspect in more detail in Section 5.1.

It is important to highlight that not all activists are equally vulnerable and "relevant" for surveillance. Administrators and platform owners are, according to Poell (2015) "connective leaders", which "invite and steer user participation by employing sophisticated marketing strategies to connect users in online communication streams and networks". He sees them as the "brand ambassadors" for the cause, and remarks that they can fall under more scrutiny than "average" activist, such as Kullena Khaled Said in Egypt under Mubarak's regime. In this case, a clear parallel can be drawn between Said and David's father and administrators of the social media accounts of „Justice for David" group. Strong use of hashtags (e.g., #jan25, #sidibouzi in Egypt, #justicefordavid in RS/BA) as well as the offline artefacts (e.g., t-shirts with slogan) can be observed for both Egypt and RS/BH protests.

Judging by the state of the art, further similarities between the activists of RS and MENA are present in the context of language, with similar ratio of activists leveraging social media using English while others use only their mother tongue. In both regions, on- and offline activities are supported by both expats and other international stakeholders, as the awareness of international community is/was "desperately" needed by „Justice for David" group, Arab Spring protesters, West Bank Wall protesters and other activist groups.

According to Mark and Semaan (2008), in Iraq "much socialization and marriage still occurs through tribal connection" (p. 145). But "by using the Internet, Iraqis now meet new people who are outside of their tribal network". In RS/BH tribal structures did not play a role before the war. However, if we compare tribes to the BH ethnic groups Serbs, Croats and Bosniaks, there are again similarities. One of the authors of this paper observed and participated in the virtual chat rooms around 1996 which were the first contact point of different ethnic groups in BH after the tragic war ended in 1995. Today, social media have an even more powerful presence in what is now an environment with relatively little ethnic diversity.

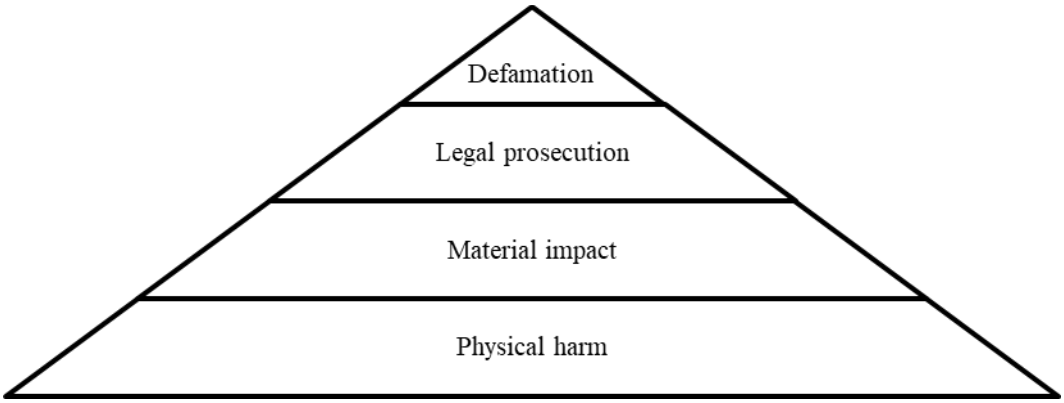
One of the Colombian FARC activists interviewed by De Castro et al. (2019), Fabio, said that "some combatants exhibited distrust towards information technology, calling it imperialist technology". At the same time Palestinian activists claim that: "…the dependency of ICT projects on international donor assistance (e.g., U.S. subsidiary firms) is rather high" and "projects funded by the U.S. impose limitations on who to hire (i.e., experts from the U.S.) and which equipment to buy (i.e., American equipment) … inhibiting long-term strategic technological developmental agenda" (Boulus-Rødje and Pernille 2019). No such comments were made by RS/BH activists, although there are relatively clear indications which media/non-profits are financed by the Western countries and which by Russia.

Numerous similarities of motive, tools, and the environment of political activism in MENA and RS/BH region hint at a similar threat landscape, in the domain of security and privacy which the authors will explore in the next section.

4.3.6 Threats for Activists Using Social Media

In this section, we will reflect on the way in which there is something, without overstating the distinction, of a difference between the way in which the "political" is coming to be construed in mature liberal democracies and how it is construed in conflictual and post-conflictual societies such as RS/BH or in the MENA region. Our point will be that in the latter instance, political action for the most part has direct consequences whereas in Europe and the USA it may take place (proportionately) at a more ideological level. This might be instantiated, for instance, in the very different ways in which privacy and security are seen to be consequential for individuals in these two different contexts. At the risk of being over-optimistic, we would suggest that there is less risk of overtly repressive behavior and deterioration into political instability in the latter. Evolving threats in the domains of security and privacy related to ICT and social media use demand simple, yet effective systematization to ensure appropriate mitigation through technological and other means. Our research pointed to common threats,

which were ranked by the estimated severity of the personal/group impact deriving from low levels of security and privacy in social media, and from which we in turn derived the "pyramidal" format (see Figure 3.). We discovered patterns in the threats, perceived and real, being faced by the activists, based on their interview statements, traditional media reports, and social media observations.



12: Threat Model Related to Security and Privacy in the Context of ICT and Social Media

Several independent interview ratings and data analyses led to ex-post facto categories concerning four abstract threat/risk levels. The categories were further elaborated in group discussions among experts. The experts e.g., counted how many times the threat was mentioned within the RS/BH interviews and compared the interviews from 2017 and 2018 with those from earlier years to identify repetitions in the mentioning of the threats and their severity. Our study offered an opportunity for a close analysis of activist concerns as directly expressed to us following occasions where activity became most pronounced (Tadic et al. 2016, 2018), from expert assessments of perceptions of threat severity, and analysis of coverage of threat in both the social and traditional media between 2012 and 2018. We also validated the initial assumptions made in RS/BH related design case study, by cross-referencing the statements of the participants and conclusions of around 20 MENA region publications conducted between 2004 and 2019. Together, this informed the structure of the threat pyramid and its applicability to the RS/BH and MENA situation. Consequences were then ranked by (approximate and sometimes overlapping) severity in relation to the security, privacy, and anonymity affordances of social media, based on one of the author's expertise in the field: defamation, legal prosecution, material impact and physical harm.

The purpose of the model, which is applicable not only to the design of technical tools, but also relates to training and awareness measures, is to:

- evoke sensitivity for potential consequences on different levels
- categorize the threats with regards to probability or potential harm/damage
- help prioritize the protection needs and enable establishment of holistic and proactive protection strategies
- frame the requirements for the design of the privacy and security solutions for the activists.

The “pyramidal” model we have devised reflects the need to heighten awareness about threat levels, not only in the current environment but also in circumstances where the political environment is, or is becoming, more unstable. On one hand, the threats for the activists in RS/BH and MENA regions are specific, as they live in fragile, often deeply ethnically, religiously, ideologically, and economically divided countries. Part of the threats related to the online space may come from the authorities (e.g., possible public service job loss due to protest participation, see statements and newspaper articles below), from private entities close to the opponents of the activists, and from individual, incentivized trolls. Content shared on social media can prompt verbal threats, insults, job insecurity, credibility loss, or ultimately even arrest. These threats can, of course, be even more severe in less stable or more reactionary contexts (e.g., torture, rape, kidnapping, lifetime in prison, similar consequences for family members). The threat model is designed to reflect possibilities in a range of contexts ranging from the fragile but as yet still relatively stable RS/BH through to the rapidly deteriorating and even dangerous contexts which are evident in some countries of MENA region and elsewhere, and which are identified by our CSCW/CHI researchers in the field. Therefore, we firmly believe that systematization, prioritization, and response measures of the threat categories for activists in this country within a single model as well as the development of the tool may be very applicable for other countries under similar and potentially worse circumstances.

4.3.6.1 Defamation

Defamation is primarily manifesting through efforts to discredit and troll the activists, either manually or automated using specialized (bot) software. Low levels of security and privacy, and exposure to social media can be correlated to identity theft and to attempts to discredit individual activists by malicious agents. The findings of Ziegele et al. (2011) also demonstrate the importance of recognizing the interrelated nature of offline and online information disclosure and implicate the need for caution in the sharing of the information in social networks that can jeopardize offline life. For example, Alena is aware of this and does not feel comfortable with her limited security. She is more concerned with identity theft that

could lead to local personal reputation damage than any legal regulation. Adam on the other hand has no fear of the authorities or his opponents but is more afraid of large-scale corporate interests. For him, security must be usable, and if it is not (e.g., being hard to understand and configure for non-experts) people will remain exposed. Brad's opinion on the consequences of self-censorship was discussed extensively by Tadic et al. (2016). Also in Egypt, it seems that "person-to-person communication was also severely restricted due to fear, and self-censorship and people often talked politics only with a few trusted family members or friends" (Tufekci and Wilson 2014). For Ela, it is important that the anonymity of her contacts and the communication in the group is protected. Also, during the „Justice for David" protests, esp. during the BH election campaign, citizens (not only activists) in Banja Luka or RS/BH were informally divided into members of the aforementioned Facebook group and non-members. The Facebook group was originally open for all, only later to become a closed group, with the team around Peter moderating the contents and approving the members. Joining a Facebook group is assumed to stand proxy for political opinion and activists in this case argue: "who is not the member of the Group, he/she is against us/the change/ justice or a supporter the regime". Comments of this kind were made by several „Justice for David" activists. Non-presence on Facebook and other social media does not, in itself, confer privacy or security. The Facebook group had around 60 posts daily alongside a high number of comments in October 2018, and some of them were images of the protesters. We can assume that some of them do not use ICT and were probably not aware that through others' posting they might be exposed to the threats (cf. De Castro et al. 2019).

Hate speech and discreditation can be observed in India in the case of Rohingya refugees from Myanmar. "Anti-Rohingya hate speech and falsehoods have since spread to India, where Facebook has 340 million users", mostly spread by "right-wing Hindu groups", according to the Goel and Rahman of the New York Times (July 2019). Discreditation example against the whole groups came from influential people such as Indian actresses, Payal Rohatgi and Koena Mitra, championed the anti-Rohingya cause on Facebook and Twitter. Ms. Mitra accused Rohingya refugees of being terrorists and criminals. Facebook removed some images posted by Ms. Mitra after The New York Times inquired about them. Also, an "extremist state lawmaker, Raja Singh, whose official Facebook page was banned in March over his anti-Muslim hate speech, set up another page weeks later. In one older video still on Facebook, he called the Rohingya 'insects' and 'worms' and said that they should be shot if they did not leave India voluntarily". Facebook stated officially in front of the US Senate that they should intensify their efforts in this context. Bloomberg describes how Philippine presidential

campaign on social media went from “groundbreaking” to turning “Facebook into a weapon” of disinformation and defamation. Authorities were seen here to methodically take down opponents, including “a prominent senator and human-rights activist who became the target of vicious online attacks and was ultimately jailed on a drug charge” and then an influential investigative journalist, after she “began probing the government’s use of social media and writing stories critical of the new president”. One of the Syrian activists interviewed in Wulf et al. (2017) “sees himself as an Internet activist who uses Facebook and Skype to inform the world about what is going on in Syria” (p. 13). A targeted discreditation campaign would permanently damage his ability to implement his vision.

One other aspect of this “discreditation” of the individuals and groups are the content policies and (mis)use of the reporting of “inappropriate” content, which leads to content removal by the social media often without discussion with those responsible for postings. One example here is the repeated Facebook removal of the pictures of David’s autopsy which Peter posted into the group. The pictures violated Facebook’s policies and after two temporary account suspensions, Peter got a warning that his account would be permanently deactivated. A second example would be the Bosniak Facebook community reporting of several links, posts and groups commenting favorably about the BH Croat general Praljak, who committed suicide in the International Court Tribunal for Yugoslavia courtroom after the first level verdict that found him guilty of war crimes (Vecernji List 2017), leading to their removal from Facebook. Palestinian activists faced similar censorship, as “a Facebook page called ‘Third Palestinian Intifada’ has been removed upon request from the Israeli government. At a similar request Apple removed the App ‘Third Palestinian Intifada’ from its App Store” (Rohde 2013, p. 3). In a society split along ethnic and religious lines, that raises the question of who and what defines appropriate content. Lots of reports of inappropriate content, whether or not they are justified (in the eyes of some), can discredit cyber activists and even lead to their banning. The arbitration of “appropriateness”, whilst recognizing its problematic character in almost all contexts, we would argue, is a somewhat more consequential matter in such fragile societies.

Ignorance of privacy aspects by activists on social media can attract (independent or politically sponsored) trolls to their online and offline “life”. At the beginning of the Arab Spring in Tunisia, according to Wulf et al. (2013b), “police of Ben Ali did not seem to be completely aware of the importance of social media nor well enough equipped to deal with it technically” (p. 1416). We believe that RS/BH authorities were also not technically equipped

to deal with the social media activities of „Save the Park" protesters in 2013. Today, the situation in both MENA and RS/BH might be different. Landwehr et al. (2019) identify the problem of "personal information bubbles, use by extremists, and the vulnerability of the political process to targeted misinformation, trolls, bots, and the like (perhaps controlled by state actors)" in regard to social networks. Networks of bots and trolls are not unfamiliar to the other parts of Southeast Europe. According to Bradshaw and Howard (2017) and Rujevic (2017), RS/BH neighbor Serbia has "a handful of dedicated employees run fake accounts to bring attention to the government's agenda" and their work is "closely monitored and reviewed by managers and leaders". In Serbia they are insultingly called "Sandwicheers" and "all they need to do is to go to formally join the party and express the wish to be activists" (Malisic 2017). They get an account for Fortress software, must use Facebook and Twitter, and their effectiveness is measured by the "point system" (e.g., 3 points for being among first 50 commenters). Coordination of human bots and trolls is done via Facebook groups. Both pro-government activists and the opposition have them. Bradshaw and Howard (2017) also deal with Iran, Israel, and Saudi Arabia. Iran has some 20,000 staff and automated fake accounts. In Israel, "cyber troops focus on positive messages that reinforce or support the government's position or political ideology" and there is "a strict policy of engaging in positive interactions with individuals who hold positions that are critical to the government" (Stern-Hoffman 2013). Sometimes, neutral comments are posted to "distract or divert attention from the issue being discussed". Bradshaw and Howard (2017) use the example of Saudi Arabia's governmental actors using automated bots for "hashtag poisoning", where "cyber troops spam trending hashtags to disrupt criticism or other unwanted conversations through a flood of unrelated tweets". Bradshaw and Howard and Hazazi (2017) claim that "Saudi Electronic Army and the Salmani Army have several members conducting campaigns on social media. These teams are often less coordinated and less formal than other cyber troop teams, but nonetheless have effects on the social media environment". (Mark and Semaan 2008) wrote that the "Iraqi government 'limited and controlled Internet' even before the war", which made activists to resort to face-to-face activity (p. 146). According to Trombetta (2012) and Gyöngy (2019) "Syrian authorities also opened an Internet platform on which the 'false reporting' of media activists has been denounced… Assad regime has adapted its methods to the extent that media activists themselves have been counteracted by cyberattacks, while the activists in turn sent videos to foreign traditional media, distributed newspapers, and pamphlets, so they finally resorted to classical communication methods" (p. 46). Examples

from Syria, Tunisia and Iraq indicate that surveillance, trolls, and bots can even reduce social media use and dependence of the activists.

In the context of activism, Facebook in RS/BH is often taken less seriously due to the personal attacks experienced, e.g., Ela said that it is “not really serious to comment on the bots and fake profiles” (cf. experiences of Suárez-Serrato et al. 2016). Twitter is used for more “serious” audiences and topics. Trolling that we extensively described is still a major issue in RS/BH, especially on a national and religious basis (Tadic et al. 2016). However, not reacting to the comments and ignoring the trolls, and sometime even people with different opinions, is the preferred form of reaction of most of the activists. Adam sees trolls as an unavoidable distraction. Kevin had threats and insults via social media, mostly from anonymous and fake profiles, but suffered no physical consequences and never reported them officially to the police. Ela is “aware that privacy is jeopardized”. She received threats from people and her comments or actions seemed to lead to the rise of bot activities. Trolling can also affect family members or associates of the activist. Peter spends a good part of his day reading and responding in the Facebook group „Justice for David”. His supporters and co-moderators of the group also read messages he receives and “filter out what’s irrelevant”. They agreed to collectively ignore the trolls (both in the online and offline world during the protests), as this is “waste of energy”. The protesters believe that response only amplifies their impact, as they confront invisible accounts or provocateurs “instructed by someone”. Peter admits that sometimes it is also not possible to control his like-minded supporters who might damage the cause, as the “mass is big”. Lepa changed her attitude towards trolling over time – in the beginning she tended to react to the trolls and now she ignores them. She admitted that some of her actions have been challenged as well, e.g., using curse words when reacting to a troll, where receiving an inappropriate language warning from Facebook. Lepa also observed that the „Justice for David” group also has their own group of members that, when the protests or protesters are “bashed” in the comments section on popular websites, use “bot” approaches to produce a large number of counter-comments (“to spit” and “to open fire”) to diminish the original negative comment of the opponents.

Within fragile environments (e.g., with a conservative authoritative regime) LGBT-parents and advocates are often target of trolls and have higher privacy and security needs within what is a complex and collective responsibility shared with children, (former) partners and families (Blackwell et al. 2016). ICT solutions need to satisfy these needs, but also should not limit them when advocacy is demanded. Blackwell et al. (2016) further discusses temporal

approval, saying that most of the actors might have more concerns about their posts after several years of time distance. Our point is that, in the absence of reliable data protection rights, such as those offered by the General Data Protection Regulation of the European Union (GDPR), risks remain substantial.

4.3.6.2 Legal action

One consequence of inadequate levels of privacy and security can be legal action. There is a balance to be struck between, on the one hand, ethically motivated interventions, honestly meant verbal "faux pas" and lack of criminal intent within RS/BH activist circles, and on the other potentially serious and criminal intent (e.g., someone inciting terrorism).

Several activists claim that the 2015 RS/BH law defining a penalty for "destructive activism" on social media as a "public space", is "still there", but is not really enforced. The cases where someone was prosecuted or arrested due to the activities of the informants, such as case from Wulf et al. (2017), were not mentioned. Beginning in July 2018, Nezavisne Novine reported that an individual from RS city of Bijeljina was arrested for inciting terrorism by inviting his Facebook followers to burn down the police station in that city. According to Ela and Brad, as there were no major protests, there was no opportunity to see whether the law would be misused by the authorities. Although these interviews had been completed before the „Justice for David" protests, there are still no (published) persecutions of activists based on this law. For Adam, the authorities are afraid of external involvement and introduced the law as a preventive tool. The BH interior affairs "agency for investigations and protection" started investigating a controversial partisan blogger from RS/BH due to a tweet on "imposition of nonexistent genocide to the Serbs" (Klix 2018). Peter, however, was sued by the members of the Ministry of Interior in May 2018 for the claim that the police killed David (N1 TV 2018) and later again, for using social media to "threaten" the police officers (SrpskaInfo 2018). During the „Justice for David" protests, the RS public broadcasting service under the control of the parties in the power, allegedly used data obtained without consent from the Ministry of Interior to "finger point" one of the activists in the protests (MojaBanjaluka 2018). This action further raised awareness around the need for the protection of the personal data in RS/BH, a topic often neglected by the local population and by the activists (e.g., Kevin: "I'm aware of surveillance… and I don't care" from Tadic et al. 2022). We see a potentially positive impact of another law, the GDPR on activists in RS/BH. Although BH is not the member on the EU, the country will adapt this regulation while seeking accession to the EU. GDPR already applies to RS/BH parties dealing with the EU and

is also applicable to any party in the RS/BH which processes data about EU citizens. For some RS/BH activists (which e.g., have double citizenship) it means “right to forget” or “right to obtain the information collected around the person” which can both inform and protect them in the context of data privacy.

However, Ali, activist from Lebanon (i.e., MENA region) who was also asked to test the Cyberactivist tool by Tadic et al. (occasional paper 2019), mentioned that the reason of his arrest was information given by an informant from his closest circle. This threat is therefore significantly more relevant and explicit in the MENA region, than in RS/BH. Syrian activists got arrested for online activism. One of them interviewed by Wulf et al. (2017) got arrested “in an internet cafe in the town of Hama. At that time, he lived in Homs where it was relatively safe to conduct political activities via Facebook” (p. 11). But the city of Hama was not. When he was arrested, “the other members of his Facebook group began to hide, fearing arrest, as well” which indicates both justified fear and the real consequences of legal actions. In Tunisia, one internet activist is quoted by Wulf et al. (2013b) that “already during the first three days of the uprising a total of 200 persons, among them 60 young adults, were arrested on charges of having uploaded video materials, pictures and news of the local uprising to their Facebook accounts” (p. 1416). As a result, activists changed their approach and took more care about anonymity: “Facebook and internet users began to use nicknames instead of real names in order to protect themselves from prosecution”. We note, however, that this is also not sufficient, as contemporary tools and meta data would still enable identification of the activists, but due to the limited resources of the Tunisian authorities at the time, this was some adequate protection. However, some Tunisian activists on Facebook also shared advice on “how to build Molotovs” (Wulf et al. 2013b, p. 1416), which would have legal consequences in any other country including Western democracies. Authors note that some legal consequences might be necessary if the protests turn to reckless violence and destruction. After the protests in Egypt in 2011 began, the security services “began using Facebook and Twitter as a source of information for a counter-insurgency strategy” and “used social media alerts to anticipate the movements of individual activists” (Howard et al. 2011, p. 16). An Egyptian activist whose Facebook group “topped 300,000 people” participating in protests, Wael Ghonim was arrested. In Syria, arrested activists were asked to “give away the passwords for both of his Facebook accounts… also … other passwords” (“They asked for the password of everything”, as cited by Wulf et al. (2017), p. 12). These practices are highly questionable and can serve the purpose of data manipulation, later surveillance, discreditation

and the compromising of all people on the contact/friend lists. They can also produce material loss, e.g., in the case of business networks or sensitive intellectual property.

Many international activists that supported causes in the MENA region limited their activities due to the possible travel restrictions tied to their activism abroad. In the past, it was harder for authorities to monitor and obtain proof of those activities. If their activism is shared on social media (e.g., photos, videos), with or without their consent, it simplifies both monitoring and proof process leading to consequences. In Palestine, "international activists are highly conscious of the consequences there might be for them, for instance, at border crossing points" (Wulf et al. 2013a, p. 1987). They sometimes have to sign statements that they will not support the protests, and posts on social media can prove otherwise. As it is critical for activists to understand the environment they are moving into, such as new countries (e.g., Western countries to Palestine), they need to understand the local differences within one country (e.g., Homs to Hama).

4.3.6.3 Material impact

Under the material impact threat for the activists, we understand e.g., loss of workplace or material privileges to be central as in a fragile society and economy, they can produce existential problems for activists and their relatives. Therefore, activists located in RS/BH implicitly ranked it as more severe than legal persecutions in the context of an ineffective legal system in the country. Brad commented on "the fears of action due to the potential of job loss" in both interviews, in 2014 and 2017 and it is remarked on elsewhere, e.g., by Kurtovic (2013). According to local BNTV station, at least three participants of „Justice for David" protests claim they lost jobs or were transferred to other cities due to high exposure during the protests. Although Adam was active in RS/BH, he was "independent" in his actions and opinions, as he is not materially dependable on the sources in RS/BH by having a job in the EU. Ali, on the other hand, was having difficulties in finding a job in his country due to his political positioning, so he was working for an internationally financed non-profit organization. Also, according to the same BNTV station, David's mother, an activist in the „Justice for David" group, claimed that her water supply was cut by a neighbor due to hostility to the protests.

There are numerous references to the job insecurity in the MENA region. Ali Bassam and Reisel (2015) write that in Syria after 2011, "many businesses have shut down because of the war, while some were victimized through the acts of sabotage causing many Syrians

economic damage and loss of jobs" (p. 248). Giacaman et al. (2004) describe the "collapse of the local economy, the destruction of the institutions in which they had previously worked, or the continuation of strict siege conditions preventing them from reaching their work in other locales" (p. 288). It is reasonable, therefore, that job loss is a very real material consequence for activists in some locations.

In the "digital age", material impact can be inflicted on activists by limiting or denying them access to the Internet. Quoting the article 19 of the Universal Declaration of Human Rights: "Everyone has the right to freedom of opinion and expression; this right includes freedom to… seek, receive, and impart information and ideas through any media". In the MENA region, besides the ban of the social media and instant messaging platforms mentioned in the previous section, Wulf et al (2013, 2015, 2017) have observed both the limitation of the individual rights to network access (e.g., in Syria), but also limitation of rights of the whole regions or groups (e.g., in Palestine, Syria). This limitation has been done through direct means such as a connectivity cut, equipment confiscation, traffic or website blocking in Syria, Iraq or Tunisia, and legal acts or indirect means such as prolongation of time taken to enable 3G connectivity in Israel for Palestinians, or Internet speed reduction in Tunisia (which prevented spread of activist videos). Howard et al. (2011) describe how Mubarak "shut down telecommunications systems… to choke off Internet access" (p. 16). The most affected were "middle-class Egyptians, who were cut off from Internet service at home", staying at home, "isolated and uncertain about the status of their friends and family". Wulf et al. (2013b) describe how in Tunisia, the authorities tried "to suppress and obstruct the information flow between local internet activists… to reduce the speed of data transfer by manipulating and pressurizing the local provider. Thus, it took a long time to upload video materials to Facebook accounts" (p. 1416). Lost access was compensated by leveraging cooperation with colleagues abroad. Tunisian cyber activists sent "the material abroad via email in a low resolution, often to friends in France, and to ask them to upload it for public use". Wulf et al. (2017) interviewed Syrian activists claim that "Facebook, Twitter and even Skype activities were surveilled and used to identify political opponents. Early on, individual accounts were blocked, and later on oppositional cities or regions were cut off from telecom infrastructures as a whole" (p. 15). This is confirmed by Gyöngy (2019) who suggested that under war conditions in Syria "restrictive measures prevented widespread Internet usage by civilians and the new media have thus lost their potential mobilization function on the ground" (p. 48).

Usage of Internet and social media in Tunis and Iraq during the "physical" curfew induced during the wartime, enabled group communication, organization, and awareness. In that context, physical limitations were not transported into the virtual world. However, in our estimation it is only matter of time until this area becomes regulated, with authorities imposing a kind of "digital or social media curfew" and having the technical capabilities to enforce these limitations. It was even, although for other motives, proposed in the UK for the children's use of social media at night (Grazia 2018).

4.3.6.4 Physical harm

During the „Justice for David" protests in 2018 in RS/BH, Peter was confronted with direct threats to his life on several occasions, mostly via social media ("death by the sniper" in a comment on a blog article by Vaskovic in July 2018 and "death by the grenade launcher" threat on social media in October 2018 according to the newspaper Nezavisne Novine, but RS/BH police apprehended both suspects). RS/BH police reacted to the threats and apprehended the persons that made those threats. Although she does not want to be anonymous, Lepa "deleted her last name from Facebook identification replacing it with a nickname because of her parents" who live in RS/BH and might face the consequences for her engagement (ranging from physical harm to discreditation). Brad claims that many people from the "dark structures" of (post)war time in BH "also occupied the authority-related structures" and are therefore a physical threat for the activists. We also observe that trolling, which is not ignored by the affected activist, can potentially also "spill" from online to offline space.

To produce a global threat model, with concomitant tool and awareness measures, we looked at MENA cases, where the threat of physical harm is more immediate. We spoke to Ali from Lebanon for an understanding of his experiences in such a case, and examined the existing literature (e.g., Shklovski et al. 2018). After being discovered as an activist, working for an international NPO, Ali was forced to leave his family and exile himself from Lebanon. Based on the messages from the authorities and their intelligence structures, Ali claims (paraphrased): "in case of my return, I would be executed. In case I continue my activism from abroad, my family will be executed". Our point, again, is that physical and material threats, while they may vary, remain significant. Shklovski and Wulf (2018) claim that (un)wanted digital visibility due to the vulnerabilities of the telephony infrastructure "can have significant and even life-threatening consequences" for activists (p. 396). Also in Colombia, many of the high-level FARC soldiers were targeted due to the possession of the

ICT equipment, and most of the lower-level soldiers and even nurses were not aware that they were in lethal danger (cf. De Castro et al. 2019).

Two of the brothers of one Syrian activist that was interviewed by Wulf et al. (2017) were killed. They became politically active after his arrest and "organized demonstrations and an uprising" (p. 12). He alleged (physical) mistreatment during his imprisonment. There was also a Palestinian activist "held in prison while another brother has been killed by Israeli forces" according to Wulf et al. (2013a, p. 1986). Still, all arrests mentioned in that paper are related to offline protest participation, and not social media activities. Relating to the Egypt's protests against the Mubarak, Howard et al. (2011) describe the case of Khaled Said, "young blogger whom police had beaten to death for exposing their corruption" (p. 15). Afterwards, Wael Ghonim, a regional executive at Google, opened the Facebook group "We are All Khaled Said" that memorized the killed blogger. Thanks to the group, that became "a portal for collective commiseration", and an image of Khaled's bruised face taken as his body lay in a city morgue passed from one mobile phone to thousands. Images of Mohamed Bouazizi from the hospital which was "passed over networks of family and friends in Tunisia" and images of David Dragicevic were spread by RS/BH „Justice for David" (Facebook) group (Tadic et. al, occasional paper 2019).

One other aspect is that surveillance might also have a positive effect such as preventing or proving physical harm. Peter from RS/BH stated that the authorities "did not want" to use triangulation to locate the movements of David's mobile phone prior to the tragic events, "deleting them on purpose". Having a secure ICT system in place, which would prevent or irreversibly document the deletion (compare distributed public ledger technologies, and effects they might have on CSCW, (cf. Prinz 2018), the family and „Justice for David" group would know where and when he disappeared.

4.3.6.5 Limitations of the model

We are aware that personal circumstances or geographies might influence the order of the layers above that of physical harm. This is based on various statements from our interviews: Lepa (being relatively well materially situated) considers discreditation to be more serious than material loss. Adam, living in the Netherlands, but being active in RS/BH has less concern that he will lose his job due to social media exposure. For the activists living in fragile societies, due to the belief that the legal system is ineffective, prioritization is generally given to the threat of material impact. One may also claim that due to the high number of

suicidal attacks in the MENA region compared to none in RS/BH in the last decades, even physical harm might be less threatening and positioned differently in the "pyramid" for MENA compared to RS/BH activists. The model above is therefore flexible and, in our example, tuned to the situation of the activists in the fragile and potentially unstable societies we are mainly concerned with. Still, even with certain current limitations, the model clearly supports evolution of the technical design prototyped and published in 2018 (cf. Tadic et al. 2018). It aims to provide a comprehensive and flexible resource for activists who are otherwise unclear about the wide range of threats they might be exposed to, providing concrete examples, clear definitions and proposals for remediation.

4.3.7 Practical Implications of Threats and MENA Aspects

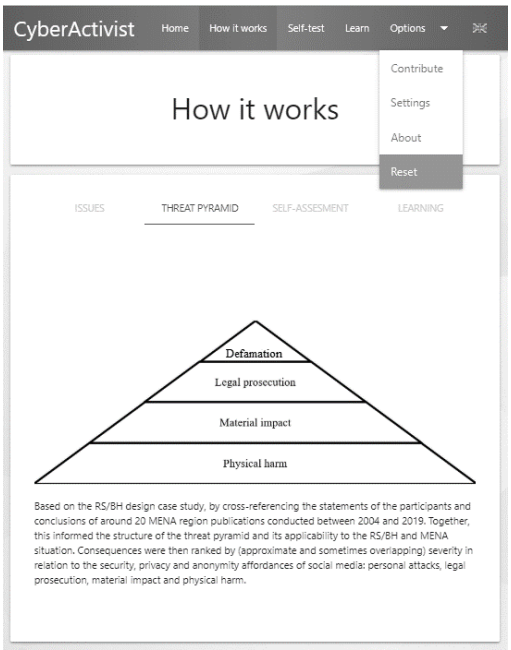
The Cyberactivist tool based on the two rounds of content analysis and semi-structured interviews with RS/BH activists and additional RS/BH activists and CHI/CSCW researcher done by Tadic et al. (2016, 2018, occasional paper 2019) can be further improved based on the results from the comparative analysis of the MENA region, as well as the links to the threat "pyramid" layers (screenshot of the current prototype: Fig. 13).

The threat "pyramid" became a part of self-test and suggested reading sections of the Cyberactivist tool. It is mapped to each question and to reading material, giving suggestions to the user as to what risks exist and can be mitigated by addressing the knowledge map (e.g., "You (or people from your environment) can get discredited/persecuted/hurt by enabling settings of this social media feature… applying this advice reduces the chances of that happening"). The threat pyramid is an evolving and localized model – after the practical, prolonged use of the Cyberactivist in which it is embedded, with the explicit consent of the users, further adaptations of the threat pyramid based on the actual tool usage are also possible.

Cyberactivist is available in English and Serbo-Croatian, and its translation in into Arabian, Farsi and Hebrew is planned with the support of the activists. The tool now enables simple integration of text files with word pairs to add new languages. The authors plan to translate the website and social media sites also to other MENA languages to speed up adoption. After the initial consequences of surveillance and oppression related to their social media activities, Tunisian and Syrian activists declared a "zero trace" approach, meaning that they reduced or anonymized their social media visibility/trackability. Wulf et al. (2017) quotes the Syrian activist and their "declared goal was to leave 'zero trace'. As soon as one Facebook account was shut down by the authorities, a new one was opened under another name" (p. 1416). On

one hand, Cyberactivist instructs users on how to increase anonymity, and on the other hand, offers the option to be used offline (e.g., copied from a memory card or downloaded over encrypted connection from the cloud). This would also prevent the unavailability of the tool, if the hostile authorities would block the website or the app download, or relevant companies banned it from the "app store".

In terms of practical recommendations, Cyberactivist, as an awareness tool and tool for self-learning, would, we argue, be well complemented with "auto config" tools which perform auto-configuration of used social media (e.g., disabling advertisement trackers on Facebook), as well as with "alternative app advisor" tools which advise on the software alternatives to popular platforms (e.g., suggesting fully encrypted Telegram IM client instead of WhatsApp). An example of an auto-config tool is the Privacy Manager and of an "alternative app advisor" is AlternativeTo.



13: „Pyramid" in the Tool Cyberactivist

Activists using the standard anti-malware on their devices, in combination with these three tools, would be significantly safer than the activists not using them. Also, if they are running their own platforms and websites, tools such as Google's Project Shield can support their availability. However, due care is advised. Using only "safe" tools, applying a "zero trace" approach and external, especially Western, Chinese or Russian software and technology, would immediately put individuals and groups on the "to be monitored / suspicions" lists in some environments, including MENA and RS/BH. Also, most of the advanced surveillance, hacking or attack attempts would not be prevented in this way. As Wulf et al. (2013b) have

already suggested, to "better understand the role social media can play in political uprisings, more research is needed into governments' use of surveillance technologies, such as Deep Packet Inspection, and activists' counter-reactions" (p. 1416).

It is fair to mention, that there are numerous platforms that provide self-test or customizable information similar to Cyberactivist related to online privacy and cybersecurity: Deutschland Sicher im Netz (2017), Warwick University (2017), USA Federal Trade Commission (2017), Consumer Reports (2021) and TacticalTech (2021), to name a few. Link and description of these platforms are listed in the Cyberactivist. Factors that differentiate Cyberactivist are possibility of download and offline use, transparency of the source code, and strong focus on the activists (others look at the citizens or companies in general). In addition, based on the results of the self-tests, Cyberactivist lists some of the tools that provide online protection, such as VPN software, ObscuraCam (2021), Project Tor (2021) or Project Shield (2021). On the side note, it would be interesting to further research the reason why the number of similar tools such as Martus (2021) and PanicButton (2021), were retired after several years despite the lack of alternatives and community interest.

In addition to software, to address the threats mentioned in the pyramid, esp. regarding physical harm, there is a necessity to use the proper devices and tools to ensure security and privacy. For this, both RS/BH and MENA activists need to have adequate resources, skills, and "powerful" allies, which are rarely present. There are some exceptions, e.g., example of the Syrian opposition forces who got an alternative telecommunication infrastructure such as satellite phones as a donation by the "West" (Wulf et al. 2017). According to Yi and Davis, (2003), effective (computer) training is a major contributor to (organizational) performance (p. 146). If the ICT donations are not accompanied with adequate, effective training, they do not represent sustainable solution for raising the security and privacy protection of the activists.

Tadic et al. (2018) have already suggested that technical design should be accompanied by tailored training and awareness measures. Online and offline training models that could be further explored do not only include localization of the contents, adaptation of the training to the specific needs of the activists, but also to the different layers of the threat "pyramid" and (non-)presence of specific security and privacy in the (fragile) environment.

4.3.8 Conclusion

Our paper clearly points out many similarities between ICT and social media use in RS/BH described by Tadic et al. (2016, 2018, occasional paper 2019) and the MENA region described by Wulf, Rohde, Aal, and many others. They include motives for ICT and social media use, similar capabilities, know-how and tools, convergence of online and offline activism, traditional and new media, as well as activism in- and outside of the country of origin. The many and varied experiences we detail above strongly support the argument that activists are subject to a number of threats, many of which they have no knowledge of and others of which they sometimes underestimate. Even where activist communities are more aware, they often have little knowledge of what kinds of protection they can afford themselves beyond the very obvious. Differences in potential threat include social structures and legal situation, e.g., ban vs. non-ban of social media. As the security and privacy risks related to social media use are not static, the CHI/CSCW community, we suggest, should try to build a current systematic snapshot of potential threats, which we have set out to do in this paper. Based on the numerous RS/BH and MENA sources, our threat pyramid summarizes the possible consequences of defamation, legal persecution, material impact, and physical harm as a result of ignorance, exposure and lack of remediation described by (Tadic et al., occasional paper 2019). We also argue that the pyramid is applicable for other regions (such as Colombia or Ukraine) and can be used to improve the technical designs related to this issue.

On Iran, Rohde (2013) comments that “trust-building and social identification with a shared enterprise and common practice – need more time than one year to show results, especially in risky and unstable situations” (p. 2). Talhouk et al. (2019) praise the role of the non-profit organizations in Syria in “facilitating design workshops and contributing to building a trusted relationship between the researcher and participants” (p. 1585). Almohamed and Vyas (2016) also consider trust important for the participative design they conducted in Jordan. We, similarly, have had to build and maintain trustful relationships in different and shifting contexts. Over longer periods of time, especially in-between periods of publication, activities and protests often cease, and activists sometimes dissipate and become unavailable. We had several difficulties obtaining the responses from the RS/BH activists in the second and third phase of our research in 2017 (the original round was in 2014). Trust building and maintenance in the unstable environments for long-term projects is something the CHI/CSCW community has to contend with in the kinds of environment we describe. This remains a partially unfulfilled ambition in some contexts. Trust is never given unconditionally and

frequently has to be renegotiated as conditions alter. Our work is a contribution to a "trustful" environment in which activists in a variety of situations can work. It does so by providing training about threat and security, and also by providing machinery for those who wish to engage in remediation efforts. We are still in the early stages of understanding how our tool might be used in other contexts which have not been examined yet. These might include, for example, societies where there are significant ethnic or tribal divisions resulting in explicit conflict. The difficulty of long-term engagement in work of this kind also means that it is difficult to keep track of a rapidly evolving technical landscape. The "punctuated" nature of technological innovation and resultant appropriation by activists is difficult to track and is, perforce, frequently historical. One possible concept we recommend for further research is the idea of "safe places", or the provision of ICT equipment and/or software to enable Internet access for activists during the curfew or protests. Wulf et al. (2017) quote Syrian activists arrested in a Cybercafe. Could this happen if there were "cyber neutral ground" for activists to use ICT and social media offered by the transnational organizations such as UN?

Flynn (2018) writes that "opposing cyber rebellions will remain a futile effort should those believing in the power of openness hold strong" and adds that "now more than ever, one must post, tweet, and email on behalf of freedom world-wide". The authors of this paper share this view and aim to make posting, tweeting, and e-mailing "safer", through raising of awareness of the activist and CHI researcher community. We argued at the beginning that issues of privacy and security, while having important consequences for everyone, are specifically consequential in conflictual and post-conflictual situations. We have substantiated this view with reference to a "continuum of risk" which is operationalized into the threat pyramid, such that the kinds of risk experienced in different circumstances vary in terms of the severity of their consequences. We have argued that exposure is, in general, particularly problematic for activists in these societies. Allied to this, and of equal consequence, we have shown that a scarcity of resources of different kinds is equally consequential. We have, in this paper, also extended the discussion about "usable security/privacy" by providing a threat model which recognizes the particularity of threats experienced in conflictual and post-conflictual societies, something that has largely been glossed over in the existing literature.

4.4 Design Evolution of a Tool for Privacy and Security Protection for Activists online: Cyberactivist

4.4.1 Abstract

This work forms a part of a series of "on the ground" studies dealing with (post-)conflict situations, focusing on the iterative, participatory design of a tool, Cyberactivist, for protection for activists and the empirical research that led to it. Work on the development of privacy and security tools has not always recognized the fragile nature of the political processes in emerging democracies, frequent naivety about threat, nor the "occasioned" responses of activists because activism can be a "one time" endeavor, prompted by specific events. Researching political activism in Republika Srpska, we identified issues relating to the use of ICT and social media, leading to the redesign of our prototype which now raises awareness of privacy and security and supports activists by challenging ignorance, lowering exposure, and enabling remediation. We addressed "usable security" challenges to ensure simplicity of the tool and engaged with HCI researchers focused on international activism to assess the global applicability of the technical design.

4.4.2 Introduction

There has been substantial interest over the past decade and more in the implementation of usable security techniques and, alongside this, a concern with what has been called "privacy by design". Although both cover similar terrain, their focus is slightly different. Privacy by design, for instance, emphasizes the embedding of privacy protocols in software applications, whereas usable security arguably encompasses wider matters such as trust, experience, ethics, and the establishing of guidelines. HCI has made a significant contribution to these areas by emphasizing the highly contingent nature of privacy and security responses and the ecologies which inform them. Our concern is - in the first instance - specific and has to do with how one provides usable privacy and security support for a population of users who have more need than most to take privacy and security seriously. These are political activists. Our contribution is an iterative design based on a threat model derived from interviews with activists and observations of, and interviews with, political protesters. We base our work on a long-term design case study of activism in the "Western Balkans" and the iteration of a design, Cyberactivist, through the different phases of the study. Both are introduced in section two, together with the research questions this paper addresses. For convenience, we distinguish between an "early" phase, previously reported by Tadic et al. (2016), and a later phase predicated on our understanding of the changing conditions entailed in a new set of protests. Below, then, we first contextualize our work with a brief description of the situation in

Bosnia-Herzegovina (BH) and then outline the way in which we conducted our earlier study and the status of the design at that point. The third section provides an overview of the relevant literature. We discuss the relevance of both “usable security” and “privacy by design” to our work, stressing an HCI viewpoint. Here we identify key research elements, which reflect the need to represent the multi-layered nature of the critical features relevant to a wide variety of activist groups threatened by opponents, regimes, or companies. In order to produce a usable technical design, the authors needed first to understand current user attitudes and behavior in relation to perceived risks in a fragile, developing democracy. The “Western Balkans” are socially, politically, and economically one of the most challenged regions in Europe. BH, one of the fragile democracies in the region according to the European Commission (2016), consists of 13 semi-autonomous administrative units based on the constitution created in 1995. The entity Republika Srpska (RS) is the largest autonomous unit with its own executive and legislative powers covering 49% of the country. Instabilities resulting from a transitional economy, proximity to and candidacy for the European Union, low GDP, poor information and communication infrastructure, complex political and media constellations, numerous socio-political activists, and the frequency of critical events in recent years make RS, we suggest, valuable for the long-term ethnographically informed design case study research. To underline this, we identified papers which explored but also emphasized the need for further research in the social media space. For example, analysis of the Al-Huwaider campaign has shown how an individual cause evolves into a social movement in a complex online environment (Agarwal et al. 2012) and highlighted a need to “discover further pathways of knowledge to fully understand people’s cognitive and social behavior, individually and collectively, in online environments with diverse social, cultural, and political backgrounds”. In the fourth section of this paper, we briefly outline the changes in the socio-political situation since our initial study in the RS context. In section five, our methodological stance is described, predicated on qualitative assumptions and a commitment to the long-term iteration of the design. Section six then discusses changes in ICT use practices since 2016 and the observable privacy and security habits of RS activists and the relevant threats to them. Section seven derives the recommended and implemented technical design changes based on our observations and input of the activists and researchers. Lastly, we discuss some implications and the degree to which the design has a wider relevance. The research results, we argue, have implications for other regions where similar conditions apply. The final section offers a summary and suggestions for further research in this domain.

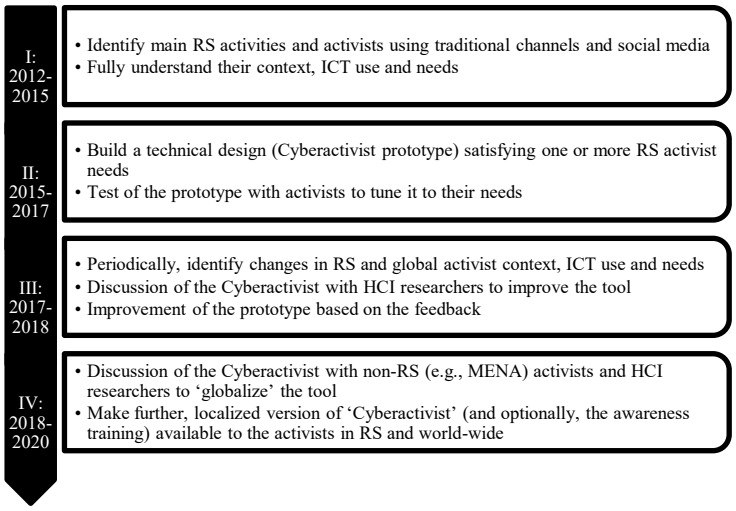
4.4.3 Long-term Design Case Study: RS Activism and ICT

Below, we describe the initial design decisions we made, and the iterations that followed in our long-term design case study. Our research questions, outlined below, reflect this evolutionary approach.

4.4.3.1 Phased Approach

According to Rohde et al. (2017), design case studies consider "the original social practices, the design discourse, the design options considered, the appropriation process, the effectiveness of the artifacts" functions and the emerging new social practices" (cf. Wulf et al. 2011; Tacchi et al. 2009; Rohde et al. 2017). Social media, activism, and security and privacy are widely covered in the research published by the HCI community, but there is, we argue, a research gap. This has to do with ICT use in emerging democracies by vulnerable populations in contentious situations. What is important about these contexts is that security and privacy issues are poorly understood and, hence, there is considerable naivety about "threat". Contentious politics, according to Tarrow (2011) occurs when, "ordinary people — often in alliance with more influential citizens and with changes in public mood — join forces in confrontation with elites, authorities, and opponents". One point to be made here is that the term "activist" might be thought to describe committed, continuously politically active people. This is, in fact, often not the case. As we shall see, in some instances at least, people become politically active, and remain so, during a specific period of contestation only. This makes long-term study more challenging, since we cannot always assume that the population of politically active people remains stable.

In the light of this, the overall research aim of our long-term design case study has to do with improvements in ICT provision for activists in emerging democracies such as RS that might be made, especially in the context of secure social media usage. The methodological commitments underpinning design case study research are described elsewhere (e.g., Wulf et al. 2015) but, briefly, entail early empirical (largely ethnographic) work, iterative (and participatory) design, further empirical investigation, and an approach to understanding appropriation. Our ongoing study follows a participatory and cyclic approach: analyzing social practices, creating, and implementing design solutions, and observing and evaluating the practices of users described in the section five. We are concerned with whether and how activists in these contexts - bearing in mind a very heterogeneous level of knowledge and experience - understand security issues and how best to support them in their political objectives in a secure way.



14: Phases of Our Long-term Design Case Study

15: "Cyberactivist" Concept

We have previously published two papers presenting the results of the phases I and II of our multi-year design case study (see Fig. 14). In the first paper by Tadic et al. (2016) we identified (at that time) prominent cyber activists in RS, providing an overview of their practices, their specific needs, and the constraints under which they act. The benefits of the use of ICT and social media by largely self-taught activists included efficient access to their target group, easier information sharing with the general population, and faster reaction to activities "on the street". Activists also faced challenges such as limited ICT know-how and resources, and low awareness regarding privacy and security. Following a series of interviews relating to protests which took place in 2015, we identified a need for a structured approach to cyber security and data privacy, locally customized ICT training, practices enhancing self-learning and knowledge transfer, and the need to act in a resource-limited environment. In the second phase of our design case study (Tadic et al. 2018), we focused on addressing these critical needs through design and implementation of an ICT prototype. Observing the RS environment, and the rising number of privacy and security issues worldwide, led us to focus our efforts on privacy and security in social media use. A technical design – named Cyberactivist – was made available for a test in a real-world situation. The initial version in the English and Serbo-Croatian languages was developed over six months in 2016, using HTML, JavaScript, and CSS, by one of the authors. It is important to provide background on that initial version to clarify where we were before the current round of investigation and redesign. The current version is then described in the section seven and the Annexes.

4.4.3.2 Initial Design

The initial tool consisted of four sections: “Self-assessment”, “Self-learning”, “Contribute”, and “My Profile”. It used easily understandable, user-centric language, reflecting the average ICT proficiency of the activists, to help them gain insight and derive appropriate actions. Two sections enabled users to understand the risks within their social media environment and to see how they were positioned regarding these risks. “Self-assessment” (see Fig. 7) contained general questions applicable to most social media platforms and questions about specific platforms, which could be answered through multiple-choice text options. The section, “My Profile” (see Fig. 9) showed whether e.g., Java is activated in a user’s browser and enables the user to set the language. The main screen showed a so called “Cyber safe score” (see Fig. 6) calculated at the time, based on the number of “plus” point and “minus” point answers from the self-assessment). Users needed to perform a self-assessment before being able to use the application’s full functionality and the main screen provided instructions on how the tool functioned. Cyberactivist also addressed resource limitations (e.g., limited training budget) through a “Self-learning” section (see Fig. 8) offering a customized array of reading materials based on the score, e.g., relating to “improvement of privacy settings of Viber”. These materials were articles published by the relevant platforms, non-profit organizations, or media with direct actionable advice on improving security, privacy, and anonymity. “Contribute” section aimed at knowledge sharing and multiplication effects, providing a non-customized list of organizations and websites providing advice to the activists, e.g., TacticalTech (2019).

4.4.3.3 Research Questions

This paper recognizes the growing importance of data privacy and cyber security in the context of ICT and social media, and identifies a mismatch between overall concerns and actual behavior (cf. the “privacy paradox”, described by Barth & De Jong 2017) as highlighted by the data collected from our interviews (Tadic et al. 2016, 2018), and answers the following questions:

- How did the activism, and related use of ICT / social media in RS, a fragile post-conflictual society, evolve since the initial research before 2016? (Sections 4.4.5 and 4.4.7)
- What are the critical issues regarding security and privacy aspects of social media use among RS, but also other activists? (Sections 4.4.4 and 4.4.7)
- How did Cyberactivist tool need to evolve to be effective and usable in addressing these critical issues? (Section 4.4.8)

In what follows, we provide an overview of the relevant, state-of-the-art literature relevant to our interest in usable security which is, more or less by definition, a subset of "privacy by design". We further discuss surveillance aspects of social media use, since it has become increasingly apparent that state and other actors have become increasingly sophisticated in their use of social media.

4.4.4 Relevant Work

Privacy by design addresses, in particular, the issue of security for non-expert users. It assumes, with some justification as our data has shown, that individuals often lack the wherewithal to make effective decisions about privacy and security. Thus, they need support. The questions raised include whether privacy and security considerations can and should be part of early development processes, whether usability factors can reduce risk, and – most pertinently for us – what specific risks attend on political uncertainty.

4.4.4.1 Privacy by Design and Usable Security

4.4.4.1.1 Privacy by Design

The literature on security and privacy is unsurprisingly extensive, given the sheer number of online attacks that take place in both the corporate and private context. As Wright has pointed out, protecting civil liberties is, at the best of times, a difficult and precarious project. Cranor and Wright (2000) argue that this is because designers have little influence over how and whether users will use systems in an appropriate fashion. Two broad and closely related, trends can be discerned in attempts to deal with this issue, these being "usable security" and "privacy by design". Such research is complicated by the complexity of interests that may be involved. Individuals and groups have certain privacy rights, whilst governments, businesses, and others have a desire to gather information about said individuals and groups. "Privacy by Design" (PbD) refers to the idea of embedding privacy protocols into technology design at the outset. This, however, is a non-trivial problem. As Spiekermann (2012) points out, it requires organizational commitment, coherent and agreed definitions of what privacy rights are to be defended, how this is to be done in practice and how to assess cost/benefit. Indeed, according to Ayalon et al (2017), the same complexities influence developers" decisions, while at the same time making it difficult for software designers to adopt PbD principles (Senarath & Arachchilage 2019). Langheinrich's influential paper (2001) points to many of the principles that should guide our privacy thinking in relation to computing technologies. Yeratziotis et al. (2012) describe the development of usable security heuristic evaluation "to test these websites

for the usability of their security and privacy features". Morton & Sasse (2012), drawing on HCI insights, have argued that privacy research has not for the most part helped practitioners, perhaps because of the complex interrelationship between hygiene factors (legislation, policy, etc.), privacy influencers (culture) and PbD principles. Drawing on Cavoukian (2009), they argue for privacy to be treated as a whole ecosystem. That thinking constitutes a contribution to Wong & Mulligan's (2019) suggestion that HCI methodological insights can contribute to an otherwise "engineering" approach to PbD.

4.4.4.1.2 Usable Security

Similarly, the research agenda around "usable security" has developed apace. Since Whitten & Doug (1999) first pointed out that users were unwilling or unable to use secure email systems, the problem of user behavior has been extensively rehearsed. Usability in this context is a significant problem because, as Birge (2009) argues, quoting Egelman (2002), "users deal with security infrequently and irregularly, and most do not notice or care about security until it is missing or broken. Security is rarely a primary goal or task of users, making many traditional HCI evaluation techniques difficult or even impossible to use". Gross and Rosson argue, in contrast, that end users do have concerns (2007a) but: "… are both unsure of the appropriate action to take and frustrated by security practices extraneous to actual work" (2007b) while Dewitt & Kulijis (2006) argue that users are typically aware of the kinds of threat posed by Internet websites but nevertheless, when confronted with a trade-off between security and usability, tend to forego security. Moreover, they are often unclear about whether security software is protecting them or not. Users, it seems, are slow, even reluctant, to engage in practices which might reduce risk. Ruoti et al. (2017) for instance, use semi-structured interviews to ascertain how users determine which security measures to adopt, and describe the various trade-offs and coping strategies that users typically engage in. Existing theory largely engages with the role of risk in decision-making, to a substantial degree based on rational choice modelling (cf. Witte 1994; Herley 2009) or, in a similar vein, cost-benefit judgments (cf. Stobert & Biddle 2014). Reasons for reluctance have been described by Ruoti et al. (2016) in a study of paired use of secure email. Abu-Salma et al. (2017a;b) has similarly examined the limitations of existing secure systems, showing that lack of user understanding, compatibility issues, and lack of motivation rooted in lack of understanding all contributed to a reluctance to use. A further difficulty is that users are not a homogeneous group. Egelman and Peer (2015) argue that too little attention has been paid to variations in user awareness and behavior and argue for increased individuation. Threat models, normally constructed by

analysts, do not always recognize the specific issues faced by certain categories of user. Hence Frik et al (2019) show how older adults exhibit misconceptions and uncertainty about security and demonstrate age specific behaviors in relation to mitigation strategies. Similar concerns come from Napoli in relation to visually impaired users (2018). Poorly designed security and privacy measures can consume significant resources without providing for either security or privacy, while others can increase security at the expense of privacy. According to the pan-European study of Friedewald et al. (2016a;b) there is no natural trade-off between privacy and security, therefore carefully designed solutions should have a spin off for both privacy and security.

To summarize, privacy and security risks, and the policies and practices which may ameliorate them, need to be considered as an ecosystem which has both socio-political elements and technological implications. As our work also shows, users in general, especially non-IT affine users often (un)intentionally neglect their security and privacy and need support in relation to levels of knowledge and awareness about these issues and their management.

4.4.4.2 Social Media and Security and Privacy

Privacy and security issues will also vary according to the technology in question. Social media, by way of example, constitute an instructive site for analysis and HCI has shown substantial interest in factors which enable better privacy and security there. Jordaan and v. Heerden (2017) identified several important privacy-related predictors of social media usage that need to be considered for the evolution of privacy models at Facebook. Long-term research by Wang et al. (2016) shows that trust had a stronger effect on individual behavior toward social media than risk, and that there are direct relations between trust objects and platform types. Trust often derives from community leaders and/or members and the platform is often secondary. Tsay-Vogel et al. (2018) examined the effects of Facebook use on privacy perceptions and self-disclosure behaviors across a five-year period. Findings point to Facebook as cultivating more relaxed privacy attitudes, subsequently increasing self-disclosure in both offline and online context and decreasing risk perception for light users. Also, the negative relationship between privacy concerns and self-disclosure weakened across time. A survey by Acquisti et al. (2006) of Facebook users found that an individual's privacy concerns are only a weak predictor of his or her membership of the network, and of the amount of shared data. Some privacy concerns were addressed by users' own ability to control the information they provide and external access to it. More surprising were the misconceptions about the online community's actual size and composition, and about the

visibility of members' profiles. There is, it appears, a significant gap between the security that is provided by systems and users' perceptions.

The study by Gaw et al. (2006) is especially relevant to our work. It looked at the behaviors of users in an organization where security was critical. Their study of ActivistCorp (a non-violent, direct action, organization) showed how personal security policies depended on social context. It carried, for instance, an overhead and was irritating to users when they were engaged in relatively trivial communication activities. This overall reluctance may be why, as McGregor et al. (2016) claim, "success stories in 'usable security' are rare". They go on, however, to describe one such success story, involving journalists dealing with the Panama paper story. They argue that a shared sense of community and purpose had an impact on the successful use of security tools, such that secrecy was maintained for a year, the whole lifecycle of the project (even though users were geographically distributed and were communicating with each other daily). As McGregor et al. (ibid) say, "we observe that project leaders also frequently and consistently articulated the importance of security measures, explicitly cultivating a sense of collaboration, mutual trust and shared security responsibility among system users". Moreover, this organizational buy-in for security measures went beyond rhetoric". Also, Friedewald et al. (2015) claim that trust in the operating institution executing the measures is an essential factor. Therefore, the technical design we are proposing for the activists must come from a trusted source. In addition, the activists often "benchmark" and help each other in the ICT context (cf. Tadic et al. 2016) and therefore optimism might be "transferred". They also have similar attitudes to those described by Dourish et al. (2004). RS activists are esp. vulnerable as they are younger, with limited knowledge of privacy-protective behaviors online, and with only low-level knowledge of government policies relating to the use of online information – all three factors, Baek et al. (2014) argue, lead to comparative optimism.

Attitudes around privacy on Facebook and Twitter are different. The findings of Yongick and Yeuseung (2017) indicate that on Facebook, young users are most concerned about other users posting on their own timeline, while on Twitter, people seem more concerned about their own tweets than about other users retweeting their tweets. Different content within different posting types has varying influence on privacy concerns. Boyd and Hargittai (2010) notice "few gender differences in how young adults approach their Facebook privacy settings, which is notable given that gender differences exist in so many other domains online", and we did find some differences in the case of RS study as well.

Chen et al. (2017) found that “being an Internet scam victim mediated the effects of routine Internet activities on privacy protection behaviors and that online privacy concerns mediated the effect of being an Internet scam victim on privacy protection behaviors”. The study discovered that “Internet users tend to ignore privacy risks until they encounter monetary loss online in person” and suggested that to mitigate the threat “users need to understand how Internet scams work”. This reaffirmed in us the belief that awareness around the topics of privacy and security is important for a potentially vulnerable group such as activists, who have also mentioned (see section four) that they are afraid e.g., of identity theft. Chen et al. (ibid) also proposed focusing further research on “other common Internet routines such as social media use” which “involve the frequent exchange of information between users, which could especially increase the risk of privacy invasion”. Bartsch et al. (2016) conclude that Internet experience leads to more online privacy literacy, which fosters a more cautious privacy behavior on social media. The study found that “people who spend more time on Facebook and changed their privacy settings more frequently had more online privacy literacy” and those with more privacy literacy “felt more secure on Facebook and implemented more social privacy settings”. Time spent on Facebook and experience with privacy regulation did not increase privacy behavior directly, stressing the importance and need of privacy awareness. Baek et al. (2014) further showed that social media users tend to believe privacy infringement is less likely to happen to oneself than to others, a finding applicable to our activists. This comparative optimism can lower overall activist privacy sensitivity.

The preliminary findings of a design approach from Brennan et al. (2014) applied to a Tibetan exile community, and related to safe and secure communication practices, have also had an influence on our technical design, insofar as they have isolated some of the issues which need to be dealt with, notably the inappropriateness of the tools “for the Internet interruption”, “usable security/privacy” where “people don’t perceive themselves as having technical know-how to use the tools” or the incompatibility of language, operating system and other technical requirements. Practices of “phone and app locks, content deletion, technology avoidance, and use of private modes” (Sambasivan et al. 2018) as design opportunities for maintaining privacy on shared devices in South Asian countries (also compare Ahmed et al. 2017) were also interesting for the shaping of the tool, especially for our self-test. Acar et al. (2016) has summed up the user problem quite succinctly as being twofold: firstly, and as we have already seen, security tends to be a secondary concern for users, and secondly “more is not better”-users are inundated with unhelpful, confusing, and overzealous policies. The same authors

also point out that there is a need for a better understanding of user policies just as much as a need for improved understanding of developers' strategies.

In a nutshell, there are four elements influencing our choice of method and our technical design. As Facebook and Twitter seem to be the primary social media for many global (and for our) activists, their privacy policies have to be well represented in the awareness part of our technical design. Further, self-perception of users, their feeling of being safe is often incorrect and our tool needs to address this. The policies, even within our tool, also have to be simple.

4.4.4.3 Use of Social Media and Data in a Political Context

There is a developing awareness of the potential for (mis)use of social media platforms and data in a political context. The topic has been extensively dealt with in research publications, as well as conventional news outlet reports. The relation of the ICT use and social, political, and cyber activism is a topic of ongoing interest for the HCI research community instantiated, for example, in the "Tunisian spring" (Wulf et al. 2013a; Buhl 2011), activism in Syria (Rohde et al. 2016), Palestine (Wulf et al. 2013b; Misaki et al. 2013; Aal et al. 2014), Egypt (Buhl 2011; Al-Ani et al. 2012), Iran (Rohde 2004), Ukraine (Shklovski & Wulf 2018) and Mexico (Monroy-Hernández et al. 2013). The approach described later in this paper, we believe, would serve to provide for the surveillance detection mentioned in almost all above papers, but also to inform activists how to protect themselves. Other work by e.g., Borge-Holthoefer et al. (2015), Kow et al. (2016) or Stewart et al. (2017) has, in various ways, examined the role of social media in new social movements. Looking primarily at Spanish and US activism, Gerbaudo (2018) explores how communications and social media are utilized as means of mobilization. He also believes that "the symbolic reconstruction of a new sense of public space will continue to be of fundamental importance in the coming years", both in stable and unstable political contexts. The importance of, but also the risks of, self-learning in the domain of security is also mentioned in reference to another developing society, Ghana, where security is learned through ad hoc practices "learned by word of mouth" (Chen et al. 2014). Bonilla et al. (2015) researched usage of the hashtags against racism in the USA. She claims that social media engagement in "hashtag activism" has "shared political temporality" but also that "participation in forms of digital activism prove transformative in unpredictable ways" (which we compare with the hashtag #pravdazadavida described in the Section 4.3). More negatively, Meikle (2014) shows, in an analysis of the "Kony 2012" campaign, how the effects of a campaign very much depend on the kind of

activism invoked. Less often, e.g., in Foth et. Al. (2015), there have been reflections on how to design support for such movements (see also e.g., Dourish 2010; Lynch et al. 2016; Vlachokyriakos 2017). Researchers deCastro et al. (2019) also point out that the "technology usage in conflict situations and its effects need to be considered as embedded in a complex network of interrelations between culture, technology, geographical location and social practices".

Traditional media can be a valuable information source for activists because of their relative immediacy. This has been identified, inter alia, as a relevant matter in the use of social media for crisis and disaster management (cf. Sutton et al. 2008; Gao et al. 2011; Latonero & Shklovski 2011; Reuter et al. 2018). At the same time, the citizens of even the most developed, stable societies have a reason for concern, as demonstrated in the New York Times piece on Cambridge Analytica, which "harvested private information from the Facebook profiles of more than 50 million users without their permission… making it one of the largest data leaks" (Rosenberg et al. 2018). Data on individual social media activity and profiling was then allegedly used to the advantage of one of the candidates in U.S. presidential campaign in 2016. Surprisingly, although Baum et al. (2019) find that "targeted product and political ads are judged more negatively than respective untargeted ads", 300 Mechanical Turk respondents do not exhibit, "a higher level of privacy concern with regard to targeted political advertising in comparison to targeted product advertising". Why this trust level remains relatively high, especially in the light of so-called "fake news", remains unclear, though some evidence suggests that this is because of people's unwillingness or inability to detect deception, or their willingness to discount it (e.g., Levine et al. 2006; Ehrlinger et al. 2004; or Gilovich 1991).

Based on research into ordinary citizen formation of political opinions, Kou & Nardi (2018) suggest design implications for supporting complex mediation, because "the echo chamber effect", leading to reinforcement of one's own opinions through likeminded people in Internet and social media, has become of increasing concern. One of the design implications suggested is "self-constructed heterogeneous networks" where, "a system that collects and ranks available VPN software is helpful to citizens who want to hide their internet position or circumvent censorship". Over 40 million Iranians use Telegram, as one of the approaches to circumvent Internet and social media tool bans (Khodabakhshi 2018).

It is clear, then, that activists today rely extensively on social media to promote and exchange ideas and activities. This has become increasingly clear since our initial design work. The

security and safety of activists in the political domain is now potentially compromised as unconventional warfare and military operations by the state have become more common (Burnore 2013) and surveillance extends into many areas beyond state intervention (Barnard-Wills 2013).

4.4.4.4 Social Media Intervention in the Private Sector

Besides pointing out the potential involvement and misuse of the social media through "extremists", "political" and "state actors", Landwehr et al. (2019) also describe the trends around surveillance capitalism and how, "most of the major IT corporations… include intensive gathering and correlation of personal information and behavioral manipulation". Uldam (2017) claims that besides well-documented government surveillance of activists, corporate surveillance of activists remains under-researched. He addresses one oil company's surveillance of individual activists who criticized the company's corporate social responsibility (CSR) program. The relation of CSR, social media and activism is also discussed by Boyd et al. (2016). Mylonas et al. (2013) also confirm low security awareness regarding "silent listeners", in this instance focusing on the smartphone apps coming from an app repository. They show how centralized repositories of this kind constitute an attack vector for hackers and, importantly, that security in such contexts is left entirely to the smartphone user to manage. Marreiros et al. (2016) indicate that people adopt a "more conservative stance on disclosing sensitive and identifiable information, even when positive attitudes of companies towards their privacy are made salient, compared to when privacy is not mentioned". Dormant consumer privacy concerns manifest only when consumers are asked to think about privacy and hence their sensitivity to exposure to risks around personal disclosure information cannot be assumed. Such studies point to the need to raise attention and awareness within activist circles. More recently, and in passing, there has been a developing interest in the security implications of the Internet of Things (Naeini et al. 2017) and the issues associated with Smart homes (Zheng et al. 2017). The New York Times also describes how smart home technology such as cameras, toys and thermostats can be easily harnessed for surveillance, misuse, or domestic violence, by the individual, and possibly by state or corporate elements (Bowles 2018). Shared photos and videos on social media and the cloud" often involve more than one social media user. If their privacy preferences are different, a less concerned user might (un)intentionally jeopardize other users by posting controversial content. Awareness of such issues, we suggest, is appreciably more important for activists in conflict-zones. Such and Rovatsos (2016) propose "a negotiation mechanism for users to

agree on a compromise for these conflicts" which "produces results fast enough to be used in actual social media infrastructures with near-optimal results".

The increase in surveillance possibilities by state and other actors, as described above, influenced our redesign. It is increasingly clear that ICT / social media users know too little about surveillance apparatuses and activists in fragile societies are both more targeted and more vulnerable. We need, then, to know more about the fragile and changing RS context in order to address this problem.

4.4.5 Changes in the RS Context

Although we have previously described the situation in RS (cf. Tadic et al. 2016; 2018; 2019), the situation has continued to change, and developments are summarized below.

4.4.5.1 ICT and Social Media Use

Much has changed in recent years in relation to the uses of social media for "political" purposes. We italicize "political" deliberately for how the term is constituted has itself been subject to change and contestation. Ranciere (2015) claims that a demonstration, "is political not because it occurs in a particular place and bears upon a particular object but rather because its form is that of a clash between two (parties)". Redolent of the "Save the Park" protests from 2013, the protests have evolved to reflect the belief that corruption is the "standard" issue in the RS (cf. Tadic et al. 2016). BH voting turnout is low (54% in 2018) according to IDEA.INT (2019) with declining numbers over the last two decades. It is often an indicator that the electorate "wants the significant change but faces the choice between two or three parties that hardly differ from each other", according to McCarthy & Wright (2015). Internet applications are important supports for civic engagement and public participation. It is not surprising, that the vernacular, critical voices in RS are therefore strongly expressed through social media and complemented by public gatherings. Our research, and that of others, points to similarities to other political contexts and to many security and privacy risks related to social media use. It also provides an insight in the lack of user engagement in practices which might reduce this risk, mostly due, not to their unwillingness, but to the (inappropriate) design of "usable" security and privacy tools in contexts such as those we describe. As all elements we outline impact our interpretation of the "on-the-ground" work and the design of our technical solution, we deal with them in the following subsections.

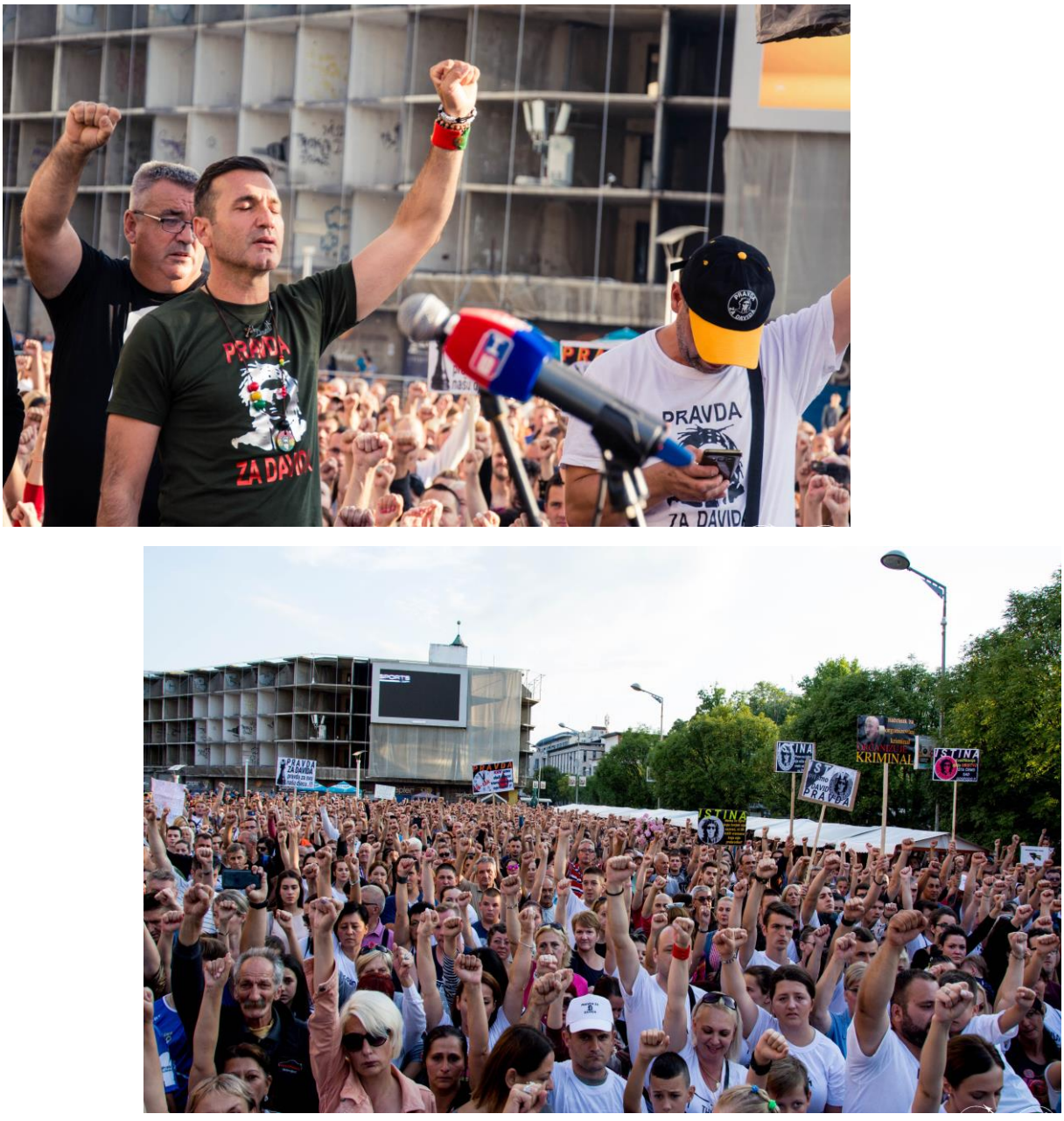
We offer a condensed overview of the local ICT situation and the major activities which surround it to better understand the privacy and security risk landscape for the RS activists.

Since our initial research in 2013, Internet World Stats (2021) reports an increase in Internet usage (2,83 million users, 86,7%) and Facebook (1,78 million users, 54,7%) within the BH population. According to Gahagan et al. (2016), BH has lower use than other Western Balkan countries, in the domains of mobile subscription and the use of virtual social media. In addition, in our earlier work of (Tadic et al. 2016; 2018), it was found that the local research community tended to limit its work to the drivers for customer engagement on social media (Bejtagić-Makić 2013), to low use of social media in medical education (Masic et al. 2012) or generally for promotion of higher education (Smajlovic et al. 2015). Statcounter (2018) also attributes more than 97% of social media use in the country to Facebook, followed by Youtube, Twitter and Instagram, with each individually less than 1%. A study from Proeduca (2016) of over 110 BH journalists showed that 91% of them use Facebook, 83% Youtube and 67% Twitter, followed by Instagram and LinkedIn with approximately 1/3 and 1/4 penetration. Among the most active journalists and bloggers are some of the RS activists already identified by Tadic et al. (2016). The Proeduca (2016) report also claims that vast majority of journalists gather information from the Internet, which gives them easier access to contacts and helps them to find relevant information, again matching our findings from Tadic et al. (2016). 79% of BH journalists say they check whether the source is credible, 19% are not sure that the information online is not “fake”, 27% believe that social media has improved freedom of expression and 30% claim they have been trolled because of the job they are doing. According to the local radio “Sarajevo” (2018), country, regional and municipal institutions still rarely use social media for communication with citizens, with municipal institutions serving as an example (e.g., Banja Luka, capital of RS). Only 14 public administration institutions of RS, out of 84 analyzed by Drljaca and Latinovic (2017) are represented on social media and this presence is described as “nonsystematic and unstructured attempts to use these free-of-charge platforms for mass communication, but without significant impact on stakeholders”. The most used platforms are Facebook (8 institutions), then Twitter (4), YouTube (4) and LinkedIn (3). The last, publicly available, study on the use of Twitter by political parties in BH is from 2012, when only four parties, from two out of three major ethnic groups in BH, had a presence on that platform, with a relatively low number of followers according to Koruga & Baca (2012). During the 2018 election campaign, it was apparent that BH presidential candidates interacted more with citizens using social media. They had between 1000 and 110000 followers and 200 to 12000 weekly interactions according to the portal Klix (2019). The most visible, with several hundred followers, was the leading party in power in RS. Observation of the political activist social media presence

regarding the elections for the BH and RS level in the autumn of 2018 shows an increase in propaganda, fake news, bots, and trolling, and our data reflects that.

4.4.5.2 “Justice for David” Protests

For our purposes, what is more interesting is the rise in activist responses when triggered by a specific event (cf. Wulf et al. 2013). After the years of relative activist “silence” after the big protest “Save the Park”, that Tadic et al. (2016) reported on, there was a resurgence with the “Justice for David” protests, an action with a high degree of regional relevance (see Fig. 16).



16: Pravda za Davida” (eng. “Justice for David”) Protests in RS Capital City of Banja Luka (Ana Radinkovic 2018)

This started after the controversial disappearance of 21-year-old student in the major city of Banja Luka in March 2018. Suspicion about an "accidental death", as initially claimed by the authorities, led to public non-violent gatherings of initially dozens, and later thousands of people on the main square of RS capital Banja Luka, organized by late David's father, mother and David's gymnasium comrades. Several times RS government-supporting media have expressed alarm at the presence of Bosniak Army veterans at protests, claiming a threat to national security. The "Justice for David" protests in FBH were also generated because of similarities with a previous case of death, in the case of 21-old Dzenan, where protests were also organized in Sarajevo by Dzenan's father. (Sarajevo Times 2019). The two groups supported each other on social media. Both the "Justice for David" and the "Dzenan" can be analyzed according to the development cycle model of protests using social media described by Sandoval-Almazan & Ramon (2014). These authors suggest that in every social issue there is one event (e.g., murder, assassination, aggression) called the "triggering event" that creates a social response. The social response is then followed by the media traditional media response (e.g., newspaper, TV, radio) and viral organization of the citizens/activists, primarily on social media, spreading the information and organizing the movement. The cycle culminates in the offline, physical response consequent on their viral organization. In "Justice for David" case, we observed the triggering event, confirmed death of David and the controversial, somewhat conflicting statements of official actors (e.g., the coroner) afterwards. In turn, we saw a traditional media response, representing conflicting positions. Lastly, triggered by family and friends, followed in turn ever growing offline protests. The responses of the authority, notably the police, again produced media response and further amplified viral and offline reaction, up to the end of 2018 (Europaba 2019). Put simply, and in keeping with what we have seen in Tunisia, Egypt, Syria and other locations, reaction had been (albeit to a lesser extent) repressive, from the perspective of the protesters and the opposition. While it cannot be claimed that there is an ideological coherence to what has developed into a somewhat general critique of the "system", the protests resemble (to a degree) the so-called Arab Spring, which was triggered by specific events but became a more generalized critique of perceived inequalities. The death of David has been a powerful trigger, like the self-immolation of M. Bouazizi in Tunisia in 2010. On 25.12.2018, according to the New York Times, "police officers in riot gear stormed a protest encampment and arrested several demonstrators who had defied a ban on public gatherings" and on 30.12.2018 after a major march around the city and clashes with the police, David's father disappeared for a while, having been accused of incitement and threatening public safety (Surk 2019). Three activists

who were identified at this gathering on this day were sued by the city authorities, while in the aftermath of the escalating protests that day, scheduled New Year concerts were cancelled. The protests in Banja Luka still take place, albeit in smaller numbers, over 700 days since the initial protests, David's body has been exhumed and moved to Vienna, where protests were also recorded in May of 2019 according to Al Jazeera (2019). "Justice for David" eventually transformed into a political party wanting to "take down the regime in RS" in 02/2020 according to N1 (2020). The case has similarities to the "justice" movements in Guatemala (Harlow 2012), USA (Bonilla & Rosa 2015) or Tunisia (Wulf et al. 2013), which continuously moved between the online and offline world and followed the Sandoval-Almazan & Ramon (op cit) model.

4.4.5.3 Social Media Attention for "Justice for David"

Numerous related Facebook posts and comments led to the foundation of the Facebook group "Justice for David" (Pravda za Davida, 2018) in the early days after David's disappearance. In 10/2018, this Facebook group had over 268340 members (number visible from outside of the group) or 343401 (number visible from inside of the group according to the activist Lepa). There were 3 admins, 9 moderators and 100 posts per day on average in 01/2019, compared to 4 admins, 6 moderators and 60 posts in 10/2018. On Twitter, we estimate that there was an average of 10 tweets a day with the hashtag #pravdazadavida / #justicefordavid in that period. The Instagram community "Justice for David" launched in 04/2018 had 5340 followers and 155 contributions with an average of 400 likes per contribution and one post per day (status 01/2019). Activist usage of these platforms, Twitter, and Instagram, as well as Viber and WhatsApp, grew significantly as compared to similar protest in previous years, e.g., during the Save the Park protests in 2013 (Tadic et al. 2016). Youtube in 01/2019 also produced hundreds of (query "justice for david") in several languages. The most watched video had over 800000 views. Among the highest ranked videos were related documentaries and interviews from local television stations (including those with popstars and TV hosts). In our interviews, activists argued that, without social media coverage, the protests would not have been visible in wider RS (and Western Balkans) society. Why is this movement relevant for our results? On the one hand, activism around the "Justice for David" movement created an unexpected, opportune moment to track the changes in ICT use over time. On the other hand, some of the most prominent activists at this time, who were facing security risks and drawing international media attention for months, participated in our study. This ultimately led to more focused improvement of our understanding of activist exposure and the resultant technical

design. Mobilization in case of “Save the Park” and “Justice for David” initiatives in the RS speaks into favor of Abu-Tayeh (2018) thesis that the primary motivator of the “citizens to participate in citizen reporting platforms” is self-concern.

All in all, ICT and social media use in RS has intensified, and carries with it security implications that we wished to examine further.

4.4.6 Method

As stated in the design case study section, this paper presents the results of the third phase of a long-term design case study. Design case studies and, more broadly, ethnographic action research, as described by Wulf et al. (2011) and Tacchi et al. (2009), served as a basis for our research. Besides building and testing the technical design, Cyberactivist, together with activists (Tadic et al. 2018), we continued to apply a mix of observational and interview techniques during the later phases to understand the major changes in activities over time (Tadic et al. 2016) in RS and the degree to which local activists now use ICT. We subscribe to the view of ethnography presented by, inter alia, Geertz (1973), Clifford & Marcus (1986), and Randall et al. (2007) which emphasizes ethnography as an analytic preference, and one which allows for a variety of methods. It can, and does, entail both watching and talking to people and discovering online and other “traces” (Geiger & Ribes 2011).

4.4.6.1 “Following” Online and Elsewhere

In our case, data was collected from RS-related content on social media (e.g., popular groups/pages on Facebook, Twitter, Youtube) and websites and traditional media reports (such as public broadcasting service RTRS, TV BN, and newspaper), identifying the issues which generated most traffic. We “followed” these activities over a period to gain a picture of their trajectory. “Following” in this context means the activation of a follow feature, accessing a page or joining the group from an anonymous account, whilst remaining “silent observers”. Similarly, we sent “follow” requests to persons/accounts which had the most impact – but did not interact with them. Our observation focused on anonymity, privacy, and security aspects. The authors, at least once a week, read activist posts and event announcements, supporter, and opponent reaction (e.g., comments, likes, sharing), speed and path of information spreading etc. on both social and traditional media. Most posts were in Serbo-Croatian, but also sometimes English, German, and other languages. They contained texts, lyrics, songs, live streams, videos, photos, illustrations, and memes, as well as the reposts from other social media platforms. This analysis informed us of the activist landscape

and the recent events they were involved in and prompted various questions for our later dialogue with activists.

4.4.6.2 Conversations with Activists and Experts

In total, the amount of time invested into observation, documentation and analysis of the social media content related to RS activities between January 2016 and April 2018 amounted to 60 hours, producing around 40 pages of notes. Our interviews involved two steps. The first step involved interviews with activists and the second with HCI researchers working in the area. For the first set of interviews, we contacted all the RS activists who participated in the first phase (six activists, 500 min of recordings) (Tadic et al. 2016) and additional activists that we identified through the above-mentioned monitoring of the social media. This time, seven RS activists responded to our invitation, with two having been also involved in the first phase of our design case study (Table V).

V: Semi-Structured Interviews with the Activists

Pseudonym	Birth Year	Role	Participated in research phase	~min. duration
Brad	1980	Project Manager at RS NPO, 2006	1,2,4	140+60
John	1978	Public Relation Officer / Editor at local NPO	1	93
Olivia	1988	Deputy Editor at local NPO / online magazine	1	56
Anna	1988	Project Manager at the local NPO	1	71
Grace	1958	Head at the local branch of an international NPO	1	72
Ela	1984	Project Manager at the RS branch of an int. NPO, 2008	1,2,4	74+19
Adam	1981	Individual activist of RS origin, EU citizen and home	2,3,4	22+2
Kevin	1981	RS journalist / an individual activist	2	76
Alena	1980	Individual RS activist for disabled population	2	30
Peter	1969	Individual activist (leader) from RS	2	32
Lepa	1985	Individual activist of RS origin, EU citizen and home	2,3	40
Ali	1984	Individual Lebanese political activist	3	20

Most of them actively participated in offline and online activities around the “Justice for David” campaign. We again applied “snowballing” techniques to reach additional activists for interviews or media (e.g., protest photos) after we spoke with the initial respondents. Lepa,

for instance, introduced us to Peter who was a key actor in "Justice for David" activities. Our interviews during both steps were, loosely, semi-structured in that the questions represented some interests we had already evolved, notably in response to their early experiences of Cyberactivist. We nevertheless pursued whatever interests our respondents demonstrated (see e.g., Helfferich 2009; Küsters 2006). We made our policy on research purpose, policy on recording, anonymity, and data protection explicit. After that, basic data about each (new) activist was collected to validate the information collected in the observational part: name, organization, position, activism experience, birthplace, birth year and workplace. Our focus was broadly on changes in their ICT infrastructure, use practices and challenges, and security, and privacy aspects of their ICT use in a social-political context. Approximately five hours of material were digitally audio-recorded in Skype/WhatsApp interviews between May of 2017 and October of 2018. One activist provided an e-mail response in addition to his statement.

VI: Cyberactivist Feedback from the HCI Researchers

Pseudonym	Sex	Role / Active since	Feedback type
Stavros	M	Researcher of Greek political activism	Skype audio
Haras	F	Researcher of international political activism, e.g., Morocco	Workshop
Daner	F	Researcher of international political activism, e.g., Palestine	Workshop
Omit	M	Researcher of "usable privacy"	Written
La	M	Researcher of international political activism, e.g., Syria	Workshop
Siega	F	Researcher of int. political activism, e.g., Sudan, Uganda	Workshop
Cloude	M	Researcher of int. political activism, e.g., Tunisia, Columbia	Written
Trademark	M	Researcher of international political activism, e.g., Iran	Written
Soiram	M	Researcher of international political activism, e.g., Middle East	Written

The interviews were transcribed in the English language and comprise approximately 60 pages (Tadic et al. 2018). In addition, as RS does not have any recent recorded cases of aggravated assaults or on-going conflicts with activists, we asked one Lebanese activist to help us to better understand these aspects. This interview was in June of 2018, in English and in person. The authors clustered all ICT use related answers according to the topics (e.g., tools used, privacy and security remarks, negative experiences) and prioritized them based on keyword frequency, but also quality of the insight (one of the paper authors has extensive

practical background in security and privacy). Authors then extracted the main changes and relevant issues which we present in the next section. The interviews were the source of the requirements for the redesign of Cyberactivist. Our goal is to make the tool easily transferable into other activist environments.

For this reason, and in a second step, we also spoke with nine researchers in the domain of HCI, who were well versed in understanding the privacy/security situation of activists from Africa, Asia, South America, and Europe (Table VI). We drew on these accumulated resources to conduct a group semi-structured, non-recorded, three-hour-workshop session in May of 2018. This produced over 50 requirements for the Cyberactivist, leading to major technical and content changes. To achieve better comparison among the Balkan countries and check the wider applicability of our findings, we also interviewed a researcher in the Greek Solidarity movement in May of 2018 in English via Skype (40 minutes). Neither activists nor HCI researchers were provided with any information besides telling them that the web application is focused on privacy and security.

4.4.6.3 Precautionary Measures

The authors took the necessary precautionary measures to protect the participants during the research and publication process and for later Cyberactivist app use, leaning on the ISO 2700x norm. The aim of the study, data handling and the "anonymization-before-publication" procedure were clearly communicated to all participants before the interaction. Interviews were implemented in a safe environment with risk mitigation (e.g., via person-to-person interviews in safe, non-surveilled environments such as public parks; via unencrypted Skype before 2018, but under the then reasonable assumption that authorities cannot maintain surveillance; after 2018 interviews via end-to-end encrypted WhatsApp). Audio files and transcripts, as well as author notes are stored on an encrypted drive. No copies are available outside the author environment (incl. journal annexes and digital libraries). Results of the test use of Cyberactivist application were used solely for the purpose of awareness raising and user experience improvement.

4.4.7 Results and discussion

In this section we describe the three major issues, threats arising from social media use in this context and way they can be addressed. The findings we describe below are independent of work we have described in previous papers, except where little change has been observed (see Fig. 14).

4.4.7.1 Social Media and Communication Tools

Our first finding was that RS activists still use similar tools to those identified in the first phase of our research before 2016. Peter, as one of the key activists in the region, was/is very negative about the social media impact on the population, especially youth, describing it as a reason for "relationship unfaithfulness", "children non-communication", or the "alienating of people from nature". He got his mobile phone and apps activated by his family members and started using social media immediately after the disappearance of his son. His negative attitudes did not change, but he and Lepa said social media, especially Facebook "helped a lot" around "Justice for David" activities. Lepa also added that Facebook activity was the main reason the RS diaspora was mobilized around these protests. Facebook and Skype seem to be used consistently among all activists, although Lepa mentioned that "she does not use Skype anymore". Alena was surprised that many people do not use e-mail, but own and actively use Facebook accounts. Twitter, Viber, and WhatsApp are gaining ground, according to Peter, Ela, Alena, Adam, and Kevin. We noticed that activists often do not differentiate between Facebook and Facebook Messenger. Ela and her contacts also used Telegram for confidential information, while Peter also got introduced to WeChat. Twitter has been described by Adam and Kevin as "more serious social media", with serious reach "that sometime surpasses expectations" and Peter started using Twitter only very recently. None of the activists mentioned use of Instagram, LinkedIn, or Snapchat. These activists seem more disposed toward the social media compared to the Solidarity activists in Greece or activists in Lebanon. Stavros shared the opinion that, due to the number of seniors that participated in the protests, most of the mobilization happened though phone calls and SMS/text messages. Lebanese activists were even more "offline", focusing on live meetings and exchange of information in such circumstances, instead of social media and ICT tools. Feedback from the activists shaped the Cyberactivist "Self-test" and "Learn" sections (see Fig. 7, e.g., categories).

4.4.7.2 Traditional Media and Environment

Compared to the first phase of our study, the role of the traditional media has not changed. As all activists agreed, so called "top-down", pro-governmental and opposition news (e.g., TV, newspaper) still play a major role in RS, as compared to "bottom-up" information distributed through the new media, which is more citizen generated. This is also encountered in the MENA region (Wulf 2013a;b; 2014). Adam claims that even the well-known activists and their platforms identified by Tadic et al. (2016) have limited impact, as they cohabit with the

system: “the system needs them to defend itself through their own media against their criticism, and they need the system to approve their existence”. Alena says that the authorities and decision makers do not recognize individual activists, so they must form groups and organize in that way. Adam thinks that only a “structured approach” (online and offline) to activism brings results. Adam is sure that in RS “the impact of cyber activism is low, compared to some larger environments”. Kevin claims that there is a low ICT literacy (“even online banking is not used”) and believes that susceptibility to fake news and manipulation is high. Activists reconfirm the need and the desire for self-learning on ICT and social media topics, but do not have “… enough time due to other priorities” (cf. McGregor et al. 2016, 2017). We can generally conclude that the situation from our initial research where the (mostly younger) activists were “digital natives”, over several last years changed to a mix of “digital natives” and “digital immigrants” (see Wang et al. 2013).

4.4.7.3 Major Issues

In the context of the privacy, security, and anonymity, we discuss three major issues that we identified. These have to do with levels of ignorance, degree of exposure and the fatalism of “no remedy”. We should emphasize at this point that although the existing literature points generically to issues of this kind, it does not tell us much about the specific security and privacy issues associated with political activism, nor how best to mitigate them.

4.4.7.3.1 Ignorance

Most of the RS activists are only partially aware of possible risks. We base this conclusion on our conversations with the activists, as well as their feedback to our Cyberactivist technical design. Kevin claims that “something “big” needs to happen for people to take their online privacy and security seriously, since “[they are] still not understanding the risks of social media, which are rather new for majority of the citizens”. This statement corresponds to our findings in both phase I and III of our design case study and illustrates that level of awareness changed only slightly in the period between 2014 and today, despite the higher coverage of the privacy and security related news in the global media. E.g., Ela mentioned “hacker attacks” in 2014, but even in 2017, she admitted that she had not changed her practices in the light of this, nor sought to be better educated. This is also made visible by the fact that our interview participants were “surprised” by the information they could obtain from the Cyberactivist tool. Most of them did not know why their “Cyber safe score” was low and said that the tool was useful to them in understanding the risks from the social media landscape

and their security and privacy settings and would recommend it further. They also explicitly mentioned that they do not (or only occasionally) use "usable security/privacy" artefacts such as encryption or backup (Tadic et al. 2016) and are not generally informed about ICT security and privacy topics. Kevin even said: "I'm aware of surveillance… and I don't care", and Peter's attitude is similar. In fact, one of them asked for an "I don't care" option to answer security or privacy related questions in the self-test questionnaire of the tool. This attitude implies the need for education, perhaps by offering real world examples of risk or by providing incentives of some kind. An important aspect for a more "typical" activist who recognizes the "privacy problem" could also be the fact that privacy policies contain "vague and unclear wording so that consumers still can hardly understand, how and by whom their data is being processed and used" (Jakobi et al. 2020). Evidence on social media use in other fragile democracies demonstrates that ICT skills, and with that cyber security and data privacy skills, tend to be limited. Most of the activists, even those with better education, started using smart phones and social media only after conflict began (cf. Wulf et al. 2014; Rohde et al. 2016), which was also the case with the main activists in the "Justice for David" protests. They underwent no formal training, neither on how to optimize ICT usage and its reach, nor on specific privacy and security aspects. One Syrian activist told us that he communicates over Skype via "Airspace Internet" and knew the brand of his router but did not know, "how the network was working, for instance, whether the router communicated via a satellite" (Wulf et al. 2014). Also, there is a perception of social media tools being safer than classical fixed and mobile telephony. One Syrian activist, when asked by Wulf et al. (2014) why he used Facebook for organizing their political activities, said it was the safest way to do it. Today, there are numerous publicly available tools for social media surveillance and monitoring, both publicly available and otherwise. This partially false perception might give a false sense of security. Even beyond the social media, there is a misconception about threat. Ali believed that when he left Lebanon and formatted the hard drive of his laptop, the laptop was then "brand new", and data was not recoverable. Such a result is quite consistent with the other research we have outlined above. Even so, the threat of, for instance, surveillance by a possibly hostile state has consequences of a possibly grave nature, something quite distinct from the general threat of "surveillance capitalism" described by Zuboff (2019). Interestingly, Vad suggested that "decision-making in a democratically organized society depends on security, confidentiality, and an open exchange of opinions" (Pickl 2019). To preserve this open exchange, it is critical to complement state care for "cyber security and the preservation of digital sovereignty" with citizen and non-profit initiatives

(such as Cyberactivist), because the level of interest of political activists may not match those of the state.

4.4.7.3.2 Exposure

Activists are also unclear about the level of their exposure and that of their families, friends, and associates on social media. One of the arguments here is that all relevant RS activists that we have interviewed over time are visible on social media with relatively high levels of personal data exposure. We were able to search for and access their profiles to determine the exact level of exposure of individual RS activists, using anonymous social media accounts (e.g., not being their Facebook "friends" nor "followers"). Apart from one individual who had no social media accounts, all our interview partners from this and the prior design study phases, including several prominent RS activists who were not interviewed, had personally identifiable data and sensitive private data which was publicly accessible. This includes posts such as family pictures, videos or information about relationships and hobbies (e.g., enjoying a hard rock concert). In addition, the Facebook groups "Justice for David" and "Save the Park" (cf. from Tadic et al. 2016) had many images which had been posted by activists, some of them containing (many) other protesters who were not aware that they were on the pictures. We assume that some of them do not use ICT or are probably not aware that their pictures are online. Also, activists who posted those, mostly group, pictures often did not know they might be expose other protesters to the threats (Such & Rovatsos 2016). Similarly, Palestinian activists also chose to mix the political posts with posts of "everyday" activities and hobbies of them and their families and friends on their Facebook profile, as well as having their Facebook friends lists publicly visible. Brandtzeg et al (2010) had warned about the consequences of having "too many Facebook friends". Wulf et al (2013) also noticed differences between less privacy-sensitive or openly ignorant local Palestinian activists and more sensitive international activists supporting their cause: "the posting of photos on Facebook pages and the usage of open mailing lists were perceived as problematic by some of the participants… international participants display greater anxiety". Similarly, "The photos taken during the demonstrations are typically posted on the local activists' Facebook accounts and in their Facebook groups without seeking permission from participants… one case in which a European participant felt uneasy about having his photo being published by the local activists and asked for its removal from the Facebook site, which was done" (ibid). Rohde (2013) notices that personal Facebook pages of the activists from Al Ma'sara are, "an assemblage of materials dealing with a variety of issues such as politics, private life, music,

film, and religion". If publicly available, this opens a variety of the attack vectors to the trolls. Posts, social media share and comment features and even the web browser signatures (relevant for all activists worldwide) or mobile video metadata expose activists to a level of visibility that they are seemingly unaware of. The same applies for shared SIM cards (in UN refugee camps in Jordan, cf. Maitland et al. 2015), where shared social media accounts (e.g., Syria or Palestine) or even used/old smart phones or erased computer drives whose memory can be accessed by specialists were used. In the case of FARC in Colombia, described by de Castro et al. (2019) with "very radical asymmetry, one where the kinds of ICT and other technology taken for granted in the Western world were not available to one side in the conflict" (deCastro et al. 2019), many people realized their exposure only too late." However, some of the interviewed activists from our latest interviews do not see anonymity positively. Adam claims "anonymous cyber activities have no legitimacy". Brad claims that anonymity is the limiting factor if you want to have impact and leave a mark, and suggests that, if necessary, the use of pseudonyms can be adopted. In his opinion, there is a differentiation between two groups: those who want anonymity and privacy, potentially aiming at illegal activities and those who strive for full transparency towards intelligence services, police, or state structures. Brad and his associates therefore share everything from private phone number to reports on cooperation and financing through foreign institutions and "publicly offers a hand to his opponents". Following Brad's remark, we confirmed that most of the trolls and bots in RS are acting anonymously, which reduces their credibility (cf. Johnson et al. 2016; Gahagan et al. 2016; Suarez-Serrato et al. 2016).

4.4.7.3.3 No Remedy

Despite the role of ignorance of the security issues (and experiences vary a great deal, ranging from direct experience to secondhand accounts drawn from the media), activists also point to their limited means to protect themselves and their stakeholders. Adam is well informed about security, but this is merely since he is studying that field at university. Lepa uses only a basic PIN and password and openly acknowledges that the primary reason she is not adjusting her privacy and security settings is negligence. Kevin is using different password complexities depending on the platform (e.g., for PayPal). Ela is keen on "protecting" her sources and the communication between the members of her organization. However, almost all activists lack time for self-learning/reading (Tadic et al. 2016) about security and privacy topics, for fine-tuning the settings on social media platforms, or installing and learning to use safer tools. In addition, they lack the budget for engaging external expertise. There is, in any case, a shortage

of this specific expertise in these contexts. Ela's non-profit organization, for instance, got some external expert opinion that security and privacy levels were adequate, but they did not act upon it for the reasons given. One of the leading portals run by activists communicated in May 2018 that they were under "hacker attack 48 hours already, but don't give up", without commenting on the attack origin. However, after several unsuccessful hostile attacks, Peter stated that supporters helped him to secure his social media accounts preventing possible personal "discreditation" and disruption of the protests. Regarding the dangers of the discreditation, observation of the online debate on digital health card in Germany showed how actors produced and disseminated "information that 'distorts' a public debate from being about an ICT innovation to being about the illegitimacy of stakeholders" creating so called legitimacy-related distortion (Wessel et al. 2017). Even in the more developed markets and stable democracies, which we can observe in the case of Greek Solidarity, according to Stavros, there are many (often senior) activists that lack the skills for ICT protection, compared to the smaller number of the technically-competent. Therefore, remedy of even the known issues is not always possible.

4.4.7.4 Threats in the Context of Security and Privacy

The importance of security and privacy protection lies in numerous accounts of threat, ranging from defamation, legal persecution and material impact to physical harm related to the engagement with activism in RS, which Tadic et al. (2019) describe in detail.

There are numerous examples of defamation, and confrontation with trolls, bots, and censorship. For example, Kevin suffered insults via social media and never reported them to the police, Alena stated that she does not feel comfortable with her limited security and Ela stated that her privacy "is jeopardized", after she received threats from people. In the case of "Justice for David", trolling and bot activity was seen almost on a daily basis up until late 2018. There was extensive use of the "report inappropriate content" feature on social media leading to content removal. Lepa also experienced the inappropriate language warning on Facebook after she commented on a troll's remark. Peter experienced it after Facebook repeatedly removed the pictures of David's autopsy from the "Justice for David" group. Frequent reports of inappropriate content can lead to a ban. On the other hand, Peter also shared that he had problems controlling his large number of like-minded supporters who might otherwise damage the cause by inappropriate defamation of the opponents or non-supporters. Even the non-participation of any Facebook user from RS on the Facebook group

“Justice for David” was seen as the silent affiliation to the ruling party, which produced further accounts of online and offline defamation.

With regard to legal consequences, RS laws include social media activities as subject to potential legal action. After claiming publicly and on social media that police killed David (N1 2018) and threatening the police officers (Srpskainfo 2018) Peter was confronted with a lawsuit by the employees of the Ministry of Interior. A local newspaper (Nezavisne Novine 2018) reported that a person from Bijeljina was arrested for inciting terrorism after he invited Facebook followers to burn down the local police station. Another material concern had to with employment. Brad emphasized “the fears of action due to the potential of job loss” and it is also mentioned by Kurtovic (2013). BN TV (2018) communicated that, due to exposure during the protests, several participants of “Justice for David” had to quit their jobs or were transferred to other cities.

Several times during the “Justice for David” protests, Peter was confronted with threats to his life, communicated through social media. One person wished him “death by the sniper” (in a comment on a blog article by Vaskovic 2018) and another, “death by the grenade launcher” (Vukic 2018). Lepa changed her Facebook identification replacing it with a nickname because she was afraid that her family might face the consequences of her engagement.

Further accounts of security and privacy threats are described, categorized, and considered in our technical design, both for RS activists as well as activists from MENA and other global activist “hotspots”. When these threats are more seriously understood, we argue, social media users and activists would be motivated to change their behavior.

4.4.7.5 Addressing the Issues

One of the safest scenarios for minimizing the above issues would be not to use social media or even ICT at all. However, for the purposes of activism today, that is clearly unrealistic, considering the role that social media now plays in terms of presence and visibility, group building and dynamics, and scalability and impact of the social media for the goals of activists. For most activists, the explicitly stated benefits of the use of social media of various kinds, and especially of Facebook (Tadic et al. 2016; 2018) outweigh the potential risks in the RS environment. Another “safe” use scenario would include severely limiting the communication group, visibility settings and to use safe tools and social media, such as those described by TacticalTech (2019), Privacy.io (2019) or discussed by Marwick (2012) and Trottier (2012). However, we took into consideration the local context, where lack of

awareness means that even the major activists share family and location data publicly or do not deploy simple protection techniques (cf. Tadic et al. 2016; 2018). Both negative and positive effects of this "openness" and cyber surveillance are well described by Marwick (2012), who shows that the related impact does not differ significantly from traditional surveillance. Understanding how lack of awareness, or misjudgment of severity, played a significant role, the authors worked on both the awareness measures and the technical design to support them. In the "usable security/privacy" part of the related research section we discussed numerous obstacles to wide acceptance of security and privacy related tools and their applicability. We also saw that secure tools can be successfully utilized in smaller groups e.g., the Panama paper case by McGregor et al. (2017). However, in a controlled Internet environment, attending the online courses or training on the topic of raising privacy level or downloading the secure apps ("as soon as I download the encryption tool, I am on the radar of the regime") from the store may set the users on the authorities' "watchlist". The question how to enable education without otherwise exposing activists would require further research. We argue that the first step to achieving good levels of security and privacy lies in knowledge transfer about privacy, security, and anonymity to the activists. Adjusting social media privacy settings to high levels, use of the "secure" tools such as Telegram, but also special tools for learning such as Cyberactivist and tailored training and awareness materials can, we suggest, help increase protection levels. For these reasons, our tool was redesigned, as described in the next section.

4.4.8 Cyberactivist Tool Evolution

As described in the section two, our prototype tool Cyberactivist is the tangible product of our long-term design case study and in this paper, we focus on its significant redesign. We focus our description on the relevant improvements and changes made compared to the original version described by Tadic et al. (2018) and Section 2.2. There are three reasons for redesigning the tool:

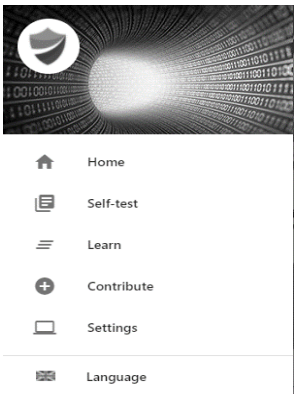
- observation of the changes in the risk landscape as described in the sections 3 and 4
- application of user-help strategies to address ignorance, exposure and no remedy for RS activists
- feedback of RS and other activists and HCI researchers on user experience of the original design.

Our solutions are not in any strict sense PbD, although they rely heavily on the notion of the ecosystem advanced by some HCI practitioners. Rather, we adopt "user-help" as a strategy.

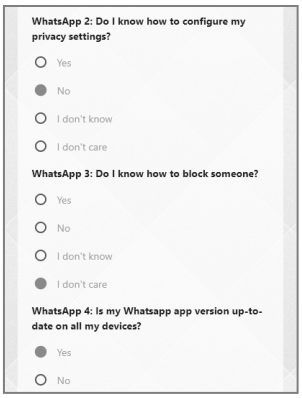
Herzog & Shahmehri (2007) analyze a variety of user-help techniques and demonstrate the strengths and weaknesses inherent in each. They ask salient questions, such is, “Is learning encouraged?”, “Is there support for performing the security task correctly?”, and “Is there a technique to prevent erroneous security decisions?”. In this section, we attempt to provide answers to such questions in the light of the feedback on features and user experience of the activists and researchers, and the need to address ignorance, exposure, and no remedy risks for the activists. We changed many of the non-functional and functional requirements, significantly improving the tool for the users.

4.4.8.1 Changes Related to Features and Functionality

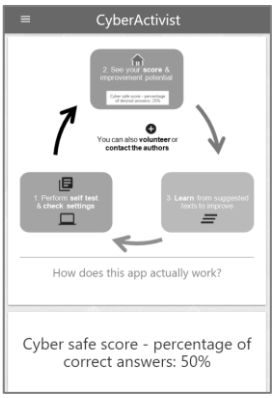
The new, post-2016 version of Cyberactivist is again based on HTML, JavaScript and CSS, extended by MaterializeCSS and Pagination.js libraries. The Web application still follows an



17: Cyberactivist Menu Listing the Sections

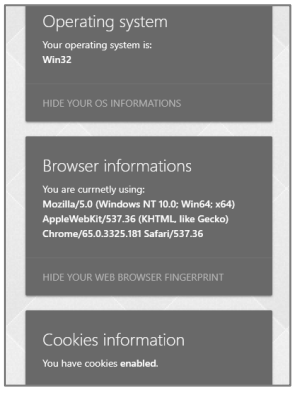


18: Self-test Section / Questionnaire

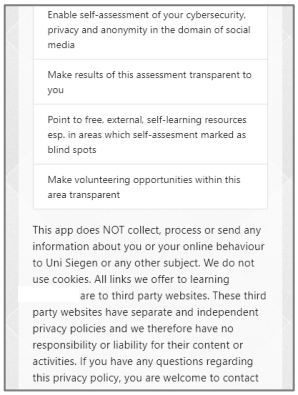


19: Revised Main Screen / Cyber Safe Score

20: Learn Section / Recommended Reading



21: Settings Section



22: About the App Section

iterative concept (see Fig. 15 and Annex III, 4.4.A.1) and consists of six, partially renamed sections (see Fig. 17): “Self-test”, “Settings”, “Learn”, “Contribute”, “About” and “How it Works”. The “Self-test” feature of the application is shown in Fig. 18. It contains more groups

of multiple-choice questions, which are now selected during the initial launch based on the social media accounts being used. Beside general questions, there are questions focusing on the specific platforms frequently mentioned by the activists (Tadic et al. 2016) with answer options (e.g., “yes” – positive answer, and “no”, “do not understand the question” and “do not care or do not want to respond” – negative answer). The selection of questions (see section 4.4.A.2), their grouping and formulation have been based on the extensive security experience of one of the authors of this paper, as well as on similar tests such as those from Deutschland Sicher im Netz (2017), Warwick (2017) or USA Federal Trade Commission (2017). In addition, the section “Settings” (see Fig. 21) still shows the data available about the user, e.g., which modules are active in the browser. The “flag” button changes the language of the application.

After the initial self-test and settings check performed by the user, the tool identifies the gaps regarding safe usage of social media though predefined conditional linkage of negative answers and reading materials. The main element of the feedback was that the purpose of the tool needs to be clearer to the user. Therefore, lots of the instructions were added in each section and the graphical user interface was made more intuitive (entailing a so-called “user journey”). In the earlier version, most activists did not understand the score or the logic of adding positive and negative answers. Therefore, the new “Cyber safe score” visible on the main application screen is now a percentage of the positive answers from the self-test (see Fig. 19). In the previous version, Kevin did not open sections “Learn” and “Contribute” as they were not intuitively displayed. A new user guide “How does this app actually work” which was asked for by several activists explains the optimal “journey” from self-test to self-learning.

Based on the score, the user obtains a personalized reading list to improve privacy and security settings in the section “Learn” (see Fig. 20). Most materials are again external articles with direct actionable advice on improving privacy and security, complemented with texts written by the authors from state-of-the-art research. In the case of a negative answer to the Instagram update question, for instance, the user would be offered the link to Instagram web page related to software updates in a separate browser window. This approach supports the preferred way of (self-)learning of the RS cyber activists, determined in large part by resource limitations. “Self-test” can be repeated at any time, to demonstrate whether the reading of the suggested materials had an effect or reset, e.g., in case of the multiple users. New features in the section “Contribute” allow users to volunteer their expertise (e.g., Brad’s suggestion of

examples for specialist IT security or video production) or ask for volunteer expert support, read about the organizations which specialize in the protection of activists or contact the authors (see Fig. 22). This simple, but logical design orientates to all topics mentioned by the activists during the participatory design process.

Different activists saw different versions, and each time authors obtained fewer improvement proposals, which combined with positive statements about the usefulness and simplicity of the tool, suggested that the development is maturing. Further questions (groups) now can be added by users through plain text configuration files (e.g., questions on TikTok or private networking). Users can also add links and texts for “Learn”, or other contribution opportunities (e.g., find a donation). The possibility to localize the interface or the section “Learn” is added to address global activists. The list of changes is available in the Annex.

4.4.8.2 Changes Related to the Issues

The tool itself is a means to protect activists and make them aware of the issues of ignorance, exposure, and no remedy. It can thus be seen as primarily precautionary and educational in its functioning. Making it more useful has to do, again, with the ecosystem referred to above. The first step is the promotion of the tool within the researcher and activist community. Quotes from the users interviewed demonstrate the need for caution by those who have suffered unpleasant consequences. An array of new elements matched to the three issues is depicted in the Annex.

4.4.7.3 Future Work on Cyberactivist

In the next months, the authors want to address the belief of the social media users that privacy infringement is less likely to happen to oneself than to others (see Section 3.2). One way to do this is by embedding up-to-date statistics on how common attacks are into Cyberactivist. The authors also recognize that adequate, tailor-made training for activists should be a parallel activity to strengthen the impact of the tool. Although we have too little data to establish whether there is a systematic “optimism bias” (or indeed associated cognitive biases such as valence and representativeness effects - see for instance Kahneman & Lovallo 1993) among RS activists, the precautionary principle would suggest that this be a feature of such training. Certainly, it is important that behavioral change be supported by whatever means can be shown to be effective. We have, as yet, paid little attention to the kinds of “nudges” that might be effective and whether a “choice architecture” (see e.g., Thaler et al. 2013) which works for most activist contexts is possible. Having said that, we are hopeful that

awareness training in some form will result in a "cascading" effect over time. Some recent suggestions include a limitation on the social media profiles of unknown persons, creation of a second account (differentiating private and professional exposure) and introduction to publicly available tools (e.g., Google Anti-DDOS protection for organizations or instant messengers for safe discussions). Another useful potential feature addressing all three issues, could be "auto-configure" (e.g., auto-configure my Facebook app for maximum security and privacy), as yet not available within the Cyberactivist due to the complexity of technical implementation. Stavros suggested starting with small steps, e.g., "how to disable cookies" in the "Settings" section, which can be turned on/off by a simple script. Considering the primary intention of the tool, to educate and protect the activists, the authors also ensured that the proposed technical design is trustworthy and safe for their use. Cyberactivist is maintained by one of the authors of this paper, who holds several global security certifications. By design, data (e.g., "Self-test" results) is stored and processed only on the users' devices using the local storage functionality of HTML and is not transmitted to any remote server. Cyberactivist is not tied in any way to any social media accounts the user might have and does not demand any account registration. It will be offered for online access via a secure server and connection in the final version, but the data will still be processed locally and possibly encrypted. In parallel, users and potential developers will be able to download and inspect the full source code, or start the Cyberactivist locally on their device, for offline use. Some links offered in the learning sections lead to third party websites, that may have separate and independent privacy policies for which the authors are not responsible. However, as also explained in the tool's "Learn" section, even with these measures, "100% security" is impossible and the motivated adversary with adequate resources (e.g., state actor) may still compromise the tool and the data.

In the next and final phase of our multiyear design case study, a web version of Cyberactivist will be made available online in several languages. Volunteers expressed their readiness to translate it into further languages and "advertise" it in the online and offline global activist communities. The source code of the application will be made available for further non-commercial development and use on the most popular open-source repositories. Other likely improvements, based on activists' comments, include further differentiation between PCs and mobile devices within the "Self-test" section; rebalancing of general and specific questions; advertising volunteer needs and availability; improving graphical representation; further improving internal security features, and potentially conversion into the native platform format (e.g., Android) for offline use. Furthermore, we plan to further optimize the user

interface applying some of the principles described by Ruiz et al. (2021). Implementation of gamification elements would also raise the attractiveness and acceptance of the Cyberactivist (e.g., La suggested, “Share a text or score with a fellow activist” feature).

In summary, all implemented and planned changes to the Cyberactivist are extensive, and from our perspective, necessary to support the wider acceptance and sustainability of the use of this tool.

4.4.9 Conclusion

The so-called “privacy paradox” refers to the way in which attitudes towards privacy seem not to be entirely reflected in behavior. Moreover, academic concerns for security, privacy and trust online seem not to be generally shared by users at large. Surprisingly, our data seems to show that there is a similar gap even when we look at the behaviors of activists, and even in situations where “background” security cannot be guaranteed. This is even more surprising when we consider that the contexts we examine are those where social stability has rapidly deteriorated in the recent past (as with Western Balkan events). We find that, although there is some relatively vague awareness of privacy threats in our community of activists, they show little detailed awareness of how these threats might manifest.

We set out three more detailed questions to be answered, the first of which had to do with what, if anything, has evolved. Based on the major events which occurred, and which prompted the reaction of activists, it seems that there continued to be no systematic concern in place regarding issues of security or privacy. Activism in RS did not seem to have changed much since our initial research in 2013-16, continuing to be a response to specific events. However, the related use of ICT and social media in RS has very much changed. As discussed in sections 4 and 5, new social media are more intensively used by the activists (e.g., Viber, Twitter, Instagram, Youtube) and many, initially tech-averse, activists started leveraging social media for their cause. Based on the “Justice for David” case, we believe that online and offline activities in RS are more intertwined than ever, both on the side of activists as well as their opponents. Regarding our second question, as is evidenced in the literature, e.g., by Marreiros et al. (2016) and Such & Rovatsos (2016) there seems to be a general indifference to, low knowledge of, or lack of willingness to confront, security issues on the level of the private individual. In the cases we describe, however, this is compounded by several factors. Firstly, levels of knowledge and expertise in our area of interest are low overall. This lack of knowledge has two aspects. Activists lack knowledge that various tools and methods are available, and they lack knowledge about how to deploy them when they are available.

Equally, high level expertise is very scarce - much more so than in more advanced economies. Secondly, material resources are very scarce. Activist groups are poorly (normally self-) funded and have no stable source of income. They are equally resource poor in relation to time. Even where there are available resources, some activists choose not to act, because they lack the awareness about the risks surrounding their engagement. Our research suggests that they need support in this context. Addressing our third question, the tool we have designed intends to provide improved support through information about the levels of privacy and security that mean that activists will be relatively safe from the kinds of harm that they might otherwise experience and, just as importantly, acts to obviate the scarcity of resources that activists in these contexts otherwise experience.

Raising awareness through simple and extensible technical design is the first step towards an appropriate protection for global socio-political activism. We have, in this paper, extended our understanding of the primary issues relating to activist use of social media, namely ignorance, exposure and lack of remediation. Secondly, we have shown that a scarcity of different resources is significantly more consequential in these contexts than it is in more advanced economies. Our point is that the kinds of motivational account, description of trade-offs, or analysis of the reasoning procedures provided in the literature hitherto, whilst undoubtedly important, are not adequate to an understanding of how activists treat security, especially in less stable contexts. In the last phase of this research, the authors plan to observe whether and what ICT use patterns by the target group change after a prolonged time of use of Cyberactivist. In addition to RS activists from all phases of our design case study, we extended the target group for participatory design to activists from other regions, such as MENA, and internationally active HCI researchers. That, we suggest, provides for some general quality, especially in the context of summarizing and structuring the threats, and ensures applicability and easier transfer of the tool to other contexts. As stated, we plan to make the tool available to activists worldwide. There are other limitations. The researchers have not paid attention to the specific security needs that some marginal groups may have. Issues of disability, gender and other identities need to be considered. HCI researchers can also complement technical design with a tailorable set of awareness measures or specialized training on privacy and security, as the knowledge gap and additional information need is identified both by researchers and by the activists themselves. For example, Xu et al. (2019) described the participatory design of similar training with urban refugees for community building. It is our intention to evaluate the value of the tool more widely, and to extend the co-creation possibilities, as time allows. In addition, the training should comprise the elements of

reaching better engagement of the citizens on social media; here activists could also leverage the learnings on practices from the industry. For instance, Hacker & Riemer (2021) show how data from corporate social networks can be utilized to derive metrics describing behavior, message content and network positions of the users.

The contribution of this paper consists of a systematic discussion of the aspects of data privacy, anonymity, and cyber security. These are topics of growing importance in the context of ICT and social media. It further extends discussions about “usable security” and PbD to consider a set of socio-political, material, and resourcing issues that have, in the main, been overlooked. The long-term study of ICT usage within socio-political activism in one region of this kind, we argue, is relatively unique and provides not only scientific insights, but also insights to – so we hope – improvement of ICT and social media usage, protection, and impact for the RS activist community. The redesigned Cyberactivist tool is, we believe, a significant step in the right direction.

5 Summary of Findings and Implications

This section summarizes the main research results from the meta-perspective and considers the implications for both activists and technical design users, and the CHI/CSCW research community and consists of four parts.

The first part describes the importance of the use of social and new media as the means to support activism and increase the reach of the activists in RS/BH. The second part focuses on the problem of security and privacy awareness among activists in RS/BH, the technical design and an initial reaction to the prototype of Cyberactivist. The third part looks at the improvements of the technical design based on the feedback of the activists and the research community, and how it addresses three key issues arising from the unsecure use of social and new media. The fourth part analyzes the potential extension of the tool to further minimize the risks clustered according to their severity and impact, ranging from defamation to physical impact.

5.1 Social Media Use by Activists

For prominent RS activists, social and new media platforms are critical instruments for communication, networking and increasing their reach. They boost the "offline" activities and enable quicker delivery of news on the relevant activities to the citizens and other interested parties. "Save the Park" protests in Banja Luka or "Babylution" in BH in 2015 which mobilized thousands of citizens were notable example of use of social media for motivating and organizing participants, sharing the news about the protests, protagonists, and societal reactions, and creating the "counter" pole to the mainstream media.

At the same time, these and similar socio-political activities pointed several challenges out. The first one was the lack of ICT and media expertise and resources to effectively manage the platforms and the content. The most activists had limited budget, limited to individual projects, and used donated equipment for which they had none or limited training. They were neither ICT-professionals nor "digital natives", therefore self-taught and, often used this knowledge to "onboard" their new colleagues. Most of the projects were very dependent on costly external IT experts. Limited resources also prevented further specialization of the roles as one person was doing several or all IT related activities. Most of the NPO sector has various, non-standardized platforms which were rarely used in the context of interoperability. Another challenge was the high dependency of the users to frequently changing terms and conditions of the platforms such as Facebook, Twitter, or Skype – e.g., Facebook policy to

pay to increase the visibility of the posts decreased the visibility of activist posts because they were not able to commercially afford paid advertisement. Due to the limited resources, activists still had challenges with the development, administration, and customization of content - and often decided to focus their resources on one or two platforms.

In addition to the need for specialized, localized, and affordable activist training - beyond basic ICT - and the need for sustainability within ICT outsourcing and use of external experts, there is a clear need for practices supporting self-learning and knowledge transfer within the RS/BH setting.

Several further implications should be considered which are loosely based on the conversation with the activists:

- Social media “premium” for free for proven non-profit or humanitarian causes
- Sharing of equipment and experts
- The attraction and engagement of more tech-savvy volunteers
- Online and offline training programs tailored to the needs of socio-political activists
- “Train the trainers” approach.

The lack of a structured approach and awareness around the topics of security, privacy, and anonymity was the aspect that caught the attention of the authors the most. Participants representing the non-profit sector and alternative media were rarely aware of the risks they are facing using social media and about the protection mechanisms (e.g., post visibility, virtual private networks, back up), or simply did not care for the potential consequences. Several of the participants of our studies and their organizations faced hacker attacks. Response to the activist activities on the social media produced lots of trolling and hate language, and some of them had to disable the commenting function on their posts. Numerous citizens decided not to engage on social media or offline media due to the possible consequences, such as loss of jobs (“Self-censorship”). Most of the activists were quite exposed using default settings of the platforms which were not protecting their privacy in the proper manner. Analog to some other countries, RS extended the law defining the consequences for activities in the cyberspace. However, mass action did not follow – state intervention was mostly limited to the individuals or groups who made threats online to the officials. In a country which struggles with corruption characterized by fragile democracy it was critical to raise awareness within this sensitive community. Most of these findings according to them activists (e.g., interview partner Adam or Kevin) are applicable to the other western Balkan countries. And even today, seven years after reaching these conclusions in our research, NPOs are exposed to rising risk -

e.g., latest attack on the activists was hostile account takeover at Buka in July 2022, causing major inaccessibility on multiple platforms, just before the release of this document and during the election campaign in BH (Buka 2022). According to Cyentia (2022) system intrusions are by far the most common and account for over half of all events and two-thirds of total losses in NPOs, with typical loss magnitude of 145 thousand USD. This need was the primary motivation for our technical design Cyberactivist.

5.2 Tool Cyberactivist for Privacy and Security Awareness

In order to address the needs of the activists beyond the theory, we decided to pursue the technical design and implement a simple, yet effective tool to raise awareness about the topics of security and privacy.

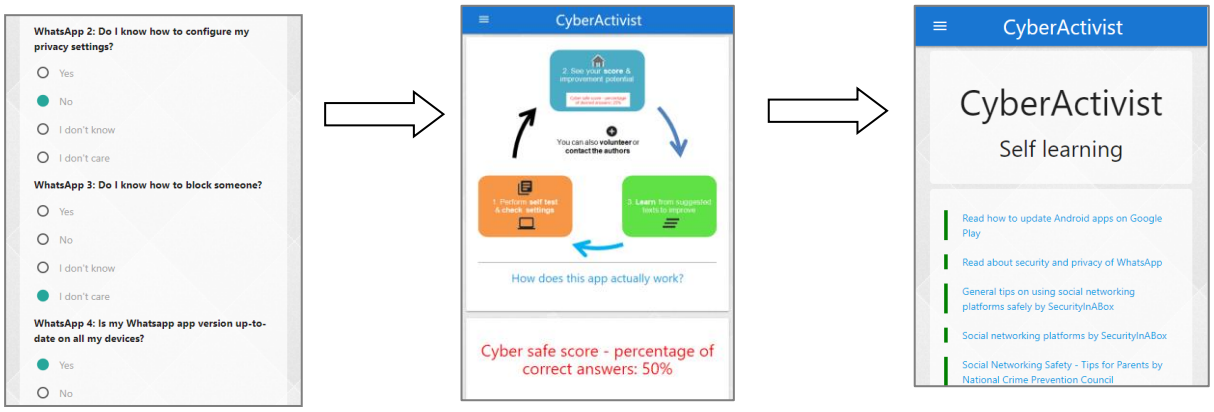
The tool Cyberactivist prototype was developed in 2016 and enables activists to understand and address the privacy and security risks related to use of social media. It is a web application based on HTML, JavaScript, and CSS code, and it includes several software components (listed in the Annex). Cyberactivist has been made “open-source” parallel to this dissertation. It can be used on- and offline, free of charge, and the source code is available for extension and modification for non-commercial purposes.

The Cyberactivist prototype was based on original technical design fit to the initially communicated needs of the RS activists and developed following the model of participatory design, as described in the Method section. Primary functions are self-assessment of privacy and security in the context of social media, and then based on the outcome, so called Cyber safe score, point to open, external learning resources and volunteering opportunities in the areas where incorrect answers in self-assessment were provided.

Learnings from the intense exchange about the initial prototype with the RS activists were building several clusters: non-intuitive interface, unclear Cyber safe score, platform customization, distribution of questions, advertisement for the volunteers (more in Section 4.4.8), translation and less technical and English terms in the translation of the tool.

Based on this feedback, we adapted the prototype to better fit the needs of activists and the community. The re-design is elaborated in Section 4.4.8.1. Besides functional and usability improvements, the author wanted to make risk/threat levels more transparent in the application. For that, thorough methodological analysis was necessary.

23: Sample Journey



1. Perform Self-test

2. See your Cyber Safe score

3. Lessons proposed based on steps 1/2, after self-learning, user can repeat step 1 or apply to volunteer

5.3 Types of Threats for Socio-Political Activists

Political activists in the RS and other fragile democracy environments around the world are frequently unaware of the risks and the potential remediation measures related to their sometimes-extensive social media use. State-of-the-art research and our interviews with researchers and activists are speaking of favor of the thesis that activism in the RS/BH is comparable to those in similar fragile democracies and regions (e.g., MENA, Central Asia, Africa, Eastern Europe, Central and South America) regarding ICT and social media use by activists. This is visible, how 4.3 elaborates, due to the similar ICT tools used, similar resource challenges and dependency of external donations, similar levels of education around security and privacy and ICT in general, as well as the improvisation and self-learning applied. Also, fewer but certain similarities are visible in the context of how the state is approaching activism online and offline.

Qualitative content analysis, empirical study and abduction based on the grounded theory described in Section 2.3 helped us derive pyramidal threat model (see Fig. 12). It offers a generalized and structured approach to the threats resulting from social and new media use in the context of security and privacy. It serves the purpose, on one hand, to motivate activists to protect themselves, but on the other hand to sensitize them using examples from different geographies about possible risks for them and their environment in case of non-protection.

The first threat layer of the pyramid is this describing defamation, hate language, and trolling in the social media. RS/BH, but also other Western Balkan countries such as Croatia (Net.hr 2021), Serbia (BalkanInsight 2020) and Montenegro (FreeEurope 2015) are also not immune to bots and fake news. Similar acts of the individuals or organized campaigns are visible also

elsewhere e.g., in India, Philippines, and the MENA region (e.g., Section 4.3.6.1). The threat is elevated by the ignorance of privacy aspects by some activists, who often (un)intentionally expose their family members, close friends, and associates. Other activists are "over-courageous" and not afraid of the threat or decide to ignore the trolling activities. Some activists limit the response opportunities, e.g., by disabling comments or by reporting to the social media platforms. Challenges sometimes arise when platforms apply ambiguous or inconsistent content blocking and filtering policies. What might be acceptable for one party, might be reported as offensive content for the other, and in the end effect, random representative of the third commercial party decides on what is "right" and what is "wrong". Some activists contribute to this threat as well (e.g., several trolls from the group "Justice for David" as the response to opponent trolling). Activists in RS also sometimes act as the promotors against the threat e.g., the strong media campaign "HEJT Sloveni" (title alluding to the hymn of former Socialist Yugoslavia with 1,25 million views by March 2022) of one of the organizations whose activists were included in this study strengthens our case, aiming at ethnic verbal violence omnipresent in the Western Balkans (BukaTV 2021). The research confirmed that there is a definite need to protect and advise activists from hate language, trolls, and defamation. Fair content filtering, maybe through one true independent non-governmental and non-profit instance, or the tools to counteract that filtering, need to be ensured. If the data has been actively used against an activist or engaged citizen, they need to have grant them right to consent or forget, such as those granted by the EU GDPR.

The second layer is describing legal action that the state or opponents to the activists are taking to limit the activist engagement or deter them. Interviewed activists claim that the 2015 RS law defines sanction for "destructive activism" in "public space" including social media is rarely enforced (see Section 4.3.6). There were several cases where the law was applied, however it was unclear whether the acts were to be seen in the context of ethical activism, as provocation to the legal state or even terrorism (details are in Section 4.3). Examples which we observed in the international context were more severe where activists were pursued and or arrested due to engagement in cyberspace. However, some of those actions are also in a gray area in the context of the legality like the protester call to "throw Molotov cocktails". On the other hand, numerous countries, especially authoritarian regimes define the laws which allow them more space in the context of pursuing and surveilling activists. That actually means their actions are justified within the national regulation however maybe morally or ethically not acceptable by the "Western standards". In addition, there is a certain differentiation in how the activists and their related data are treated if they have only local or

also citizenship of another country. There are ways to limit the visibility of the activists in the context of cyber activities, however they are not often known to the general public or actively disengaged by the state and the opposition. It is important to mention that in order to avoid the above threats (e.g., loss of employment), some citizens in RS and other regions aim to self-censor and limit their interactions on- and offline. Other activists apply their own censorship on their platforms, excluding non-like-minded individuals, opposition, or activists from the discussions, or blocking their access and content. Being informed about the legal interpretation and implications of their potential actions would prevent activists being legally exposed and prosecuted but would also demotivate being too careful around self-censorship. Cyberactivist is providing this advice and included findings can help sensitize around this topic.

The third layer speaks about the material loss and how it can affect the wellbeing and even the mere existence of the activists in economically weak societies. According to the IRB (2022), in 2020 RS and FBH economy are characterized by low GDP per capita (9795 in RS, 10181 in FBH), high unemployment (24,1% RS, 39,5% FBH) and low average monthly income (956 Bosnian Mark in both). Several RS activists mentioned that e.g., loss of workplace or source of income can produce existential problems for citizens and their relatives, and that this deters them from becoming more engaged in the civil society. This fear was not observable in the statement of activists who lived abroad, i.e., in the countries of the EU with higher standards of living, and job and social security. Also, in addition to the loss of income, in some other regions outside of Western Balkans activists lost possibility or means to access information e.g., through confiscation of equipment, Internet link limitation or content filtering (for examples, see Section 4.3.6.1). Being informed about the risks and potential workarounds could mean that activists become even more active. Also, option to use the free tools, such as Google DDOS protection, and engage volunteers, like-minded individuals, and groups through Cyberactivist could additionally ease the pressure on the income of the activists and the budgets and outsourcing needs of non-profit organizations.

Threat within the fourth layer is most rare, but most severe, as it concerns physical harm or even loss of life of the activists. Some RS activists, esp. the leader of the Justice for David movement, received life threats from non-state actors (see Section 4.3.6), however RS police reacted and there were no consequences. In some other regions e.g., MENA or South America, that threat was more present and serious (see examples in Section 4.3.6.4). Some of the consequences of the physical harm, even corpse pictures posted in the social media or

displayed offline, were motivator for the increase in online and offline activities of the activists such as in the case of Tunisia (see Section 4.3.5). One of the purposes of Cyberactivist is not only to educate the activists about possible physical harm to them and their loved ones and fellow activists, but also to do so without jeopardizing them (compare offline use). Also, by providing an appeal to inform about the legal consequences, Cyberactivist deters the potential actions that might be considered as society-endangering or even physical threat to the citizens.

There are also several limitations of the model, such as different perceptions of the importance and impact (e.g., in some cultures defamation might be more relevant than material loss).

The layer logic has also been integrated into the Cyberactivist technical design and the tool. We integrated and clustered certain self-learn content and built-in elements within the self-test according to the layer logic. In addition, authors considered adapting the Cyber safe score according to the weight of the threat that is estimated for severity by the user.

The threat pyramid is designed to evolve – after the practical use of Cyberactivist and collection of the learnings in regard to the model further adaptation of the pyramid based on the usage are possible with the explicit consent of the users. In order to minimize the threats that the usage of the tool itself produces, an offline version has been generated. This adaptation can be handled without Internet connection and therefore would be not traceable for the surveillance parties unless someone accessed the device itself.

The tool Cyberactivist can obviously be adapted for MENA or other regions and combined with other tools (see Sections 4.4.8 or 5.5) to ensure a holistic awareness and response to these threats. There is also a necessity to use the tool in the manner to address three topics in regards security which we clustered in the initial phase of our research: ignorance, exposure, and non-remediation.

5.4 Evolution of the Cyberactivist Tool

So even if the risks are known activists are unaware that they are exposed, decide to ignore them, or have no means to address them. Our examination of the “privacy paradox” – when behavior does not reflect attitudes towards privacy – produced the concerning image in the context of the activists and journalists. Our activists showed no thorough awareness of how security and privacy threats manifest. In our second round of talks with prominent activists and researchers, we experienced relative stability in terms of the tools used – which were

observed in the first round of interviews – with relatively high dependency of tools belonging to the Meta corporation (WhatsApp, Facebook, Instagram) and Twitter. Besides commercial aspects, i.e., being able to afford to publish on this platform, this dependency raises concerns esp. if we look at the company Meta and its often-controversial privacy and sharing policies. However, more citizens started using these platforms to express their discontent or sympathy for the activists and their causes. Most of the engaged individuals and groups again shared three major issues that we identified in the first phase of our research with our activists - level of ignorance, level of exposure and the challenge of non-sufficient remedy. This especially came into effect during the massive “Justice for David” protests, which connected offline and online activities in ways RS has not seen before.

We needed to motivate the activists about the need to inform themselves about the risks within security and privacy, therefore addressing the ignorance issue. Low knowledge level as well as sensitivity around security and privacy corresponds to the RS society's interest in security and privacy which is also low. However, some of the activists showed over self-confidence almost “invincibility” syndrome, which they would change if they were informed about the threat levels we described within the four-layer pyramid.

Regarding the exposure, most of the activists did not know that they were jeopardizing themselves and others by sharing without permission or with default privacy settings. For example, the protesters injustice for David case posted the picture from the protest including people which may face consequences at their work and did not know that they were shared online. However, there were also activists which wanted to keep high exposure claiming that that increases their credibility towards the public.

We also observe the issue with lack of remediation, as the ICT skills of the activists were limited - it ranged from not being able to set the appropriate password to not being able to defend themselves from DDOS attack.

In a nutshell - first, activists did not know which threats they face or ignored them; second even if they knew the “cure” they have limited knowledge or the means to apply the cure, i.e., address and mitigate the threats using even the freely available means, or even lacked any protection at all. In addition, they were facing social media platform censorship even if the content was authored by them e.g., due to political reasons, complaints of other users or automatic filtering of explicit imagery. They also had challenges managing their supporters

and their behavior online or anticipated persecution following the law defining acceptable behavior on social media.

For this reason, we decided to upgrade and extend our original technical design. Several iterations of Cyberactivist included various changes to the functionality and the features. Examples of some of the changes include the:

- Cyber safe score logic, which became more simple
- self-test questionnaire, where answer options, progress bar and categories drove usability
- extension of the learn section, where additional learning links were added
- adaptation of the settings and the GUI allowing e.g., multilingualism and easier navigation
- as well as the further help and instructions for the use of the application (see Annex).

In addition to the threat pyramid, elements related to the issues were added as well, such as contextual hints on how to deal with the issues, simplified language and the examples from the other activist communities and geographies (see Section 4.4 and Annex). A whole array of furniture potential extensions of the tool was listed in the outlook for further research and developer communities to explore. Both, this software code, and the way how it has been developed, customized and gradually improved, based on the research and user feedback are, without a doubt, some of the main contributions of this dissertation to the research at the intersection of CSCW, EAC, PbD and usable security.

5.5 Comparable Tools and Accompanying Training

Besides Cyberactivist, there are more – often free – applications that may help with awareness and education in the domain of security and privacy, as well as the actual protection. Examples are AwareEC (AwareEC 2022), thedefenceworks (thedefenceworks 2022) and LucySecurity (LucySecurity 2022). Free apps such as Bodyguard have interface for most of the social media and claim to detect “hate speech on the internet with a 90% to 95% accuracy and only 2% of false positive” (Dillet 2021). We suggest the possibility of extending or complementing the tool with adequate training. There are numerous trainings which can positively impact the activist community such as ULEX Project (ULEX 2021), focusing on how “organizations and networks relate to the wider ecology of activism” and “wider struggles in the ever changing cultural, socio-political and ecological context”, Totem Project (TOTEM 2021), that “helps journalists and activists use digital security and privacy tools and tactics more effectively in their work”, or Deutschland Sicher im Netz (DSIN 2021), that

enables “easy check of the security status” for the small and mid-sized organizations (possible comparable to the NPOs), with tailored recommendations similar to the Cyberactivist logic.

Even the biggest ICT companies are offering free cybersecurity and/or privacy training, e.g., Cybersecurity Awareness Training from Amazon (Amazon 2022). In academic circles, numerous authors inspire the further development of the training, e.g., Xu et al. (2019) describing the design of training for community building with urban refugees or e.g., Hacker & Riemer (2020) showing how corporate social networks can help describe behavior, content, and networking of the users.

5.6 How the Cyberactivist Addresses the Activist Needs

All interactions with activists and researchers, as well as the feedback from the review committees of the paper and journal contributions provided the insights into several implication which should be considered when building the tools for the engaged citizens. Designed in this way, the tool addresses the main needs of the activists and research community:

- It is intuitively built and easy to use, thanks to its “natural flow”, leading from the self-test overdone analysis of the outcome and to the recommended reading (see Fig. 23)
- The application itself as well as the content is openly available and free of charge, and therefore attractive for activists and organizations with scarce resources
- It can be run on any platform making it attractive to activists from various regions
- Its source code is fully open for analysis, as well as transparency purposes
- It is extendible easily, for people with limited software development skills, both in terms of functionality as well as the customization of the content e.g., adding reading materials
- It follows the principles of usable security and privacy and PbD protecting its users from unintentional disclosure
- It is easily adaptable to the regional specifics such as language (English and Serbo-Croatian are available). The activists can change the language label pairs, adding or modifying a plain text JavaScript file in the directory scripts/lang and then adding an option to selectLanguage function in the main code
- Due to the gamification elements (e.g., score) it fosters self-learning and -improvement
- It offers the rudimentary possibility to search for volunteers or offer volunteering.

Authors hope that the activist, research, and developer communities will further develop and enhance the tool long after this research project is completed.

6 Conclusion and Outlook

Activists and journalists around the world are facing more uncertainty and higher individual threats. Good part of the actual threat, ranging from defamation to physical harm, as our published papers elaborate, comes from the technology as well as the visibility and engagement in the social and new media space. Surveillance and interference in cyberspace have long gone from niche specialty of authoritarian regimes to the open market service "profit machine" for state and commercial actors even in the developed democracies. Company NSO from Israel, author of the Pegasus software with "zero-click" capabilities to infiltrate mobile phones (i.e., "you don't even need to press a button or follow a link for it to take over your device, at which point it can intercept text messages, track calls, retrieve passwords and access the microphone and camera" (Edan 2021)), does business with 55 countries world-wide with declared "commitment to respect human rights" (NSO 2021). Various papers (such as Edan 2021) point out NSO and Pegasus in the relation with the officials of Saudi Arabia, India, Hungary, Rwanda, and Azerbaijan, known by specific regulation related to and/or treatment of the journalists and activists.

Also, the commercial actors behind major social media platforms, as we pointed out in our Section 4.3, ambiguously decide, or allow governments to block someone or filter some content, such as example of Palestinian activists WhatsApp being blocked by the Israeli government (Al-Jazeera 2021).

This strengthens our conviction that we selected the right questions to address: how can ICT help activists, esp. in fragile societies, and boost their impact? What are their key issues? Which threats should they be sensible about? And how to protect them, in the context of data privacy and security? The process and results of design case study, as well as the tool Cyberactivist have not only answered these questions, but also produced various beneficial implications for the activists, business and public sector, and the research community.

Activists obtained a number of examples of how ICT can be better and more securely used in the when facing scarcity of resources, knowledge and/or interest. Then there is an overview of the risks and similarities over the regions (e.g., West Balkans and MENA), which can incite further learning from the experiences and exchange with the activists from other regions. Finally, a scientifically verified and localized tool Cyberactivist can easily spread and help further educate thousands of activists, involved citizens and researchers globally and help them to protect themselves, their activities, and their network.

The public sector, esp. the authorities, can also benefit from understanding better the needs of the activists and engaged citizens. This transparency can help reduce the reasons for citizen discontent, strengthen social cohesion and further support appropriate citizen engagement. The public sector can further refine the (national) legal framework to achieve both better quality of the current regulation and related instruments for the online and offline space, without reducing or suppressing the freedom of opinion. Knowledge of the activist protection mechanisms can also contribute to the optimization of the state protection mechanisms in case of destructive behavior (e.g., coup d'état).

For the business sector the results of this research enable better understanding of this specific target group and their situation. This can be then used to develop products and services tailored for this, but also other similar users (such as journalists or humanitarian workers) or even the "ordinary" citizens. Also, further development and even commercialization of the tool Cyberactivist by the business sector, as it is open source, is also possible. This can enable the business sector to expand their corporate social responsibility portfolio. However, the commercialization may also limit the protection of the activists, by e.g., disabling access to advanced features limited to paying, premium users – which most activists and NPOs are not - or e.g., in the worst case, enable access to activist data to the "regimes", if the business sector is forced into this course of action to remain active on that specific market.

The research community has obtained current and long-term ethnographic observation from a region with extremely specific characteristics for European terms – post-conflictual fragility, transition, and ethnic and other divisions. It provides not only insights on how ICT can be better utilized by socio-political activists and citizens, but also how it could be applied to contribute to peace and stability. Our research also enables the "pyramid" to better categorize and respond to the threats, which can be further refined, with additional protection measures developed. The further development of the tool Cyberactivist based on the existing, but also further independent, research is also recommended. Further development of the tool, as it is open-source software, can be done by separate developer and end user (i.e., activist) personas as described in the system design by Hellman et al. (2021). Cyberactivist can also be complemented with further audio-visual elements, such as augmented reality self-test or learning elements, which Ludwig (2021) described for troubleshooting. In the sense of the context, psychological models of Ferwerda et al. (2021) can also be considered in order to address ignorance or address the consequences arising from the threats.

Further, the researchers did not pay attention to the security and privacy needs of some marginal groups, e.g., disability or gender. For the Western Balkans, as a route for migrations to central and western Europe, activism around migrations and activism around sustainability may become very relevant soon, in addition to political and anti-corruption activism.

This long-term study of ICT usage within socio-political activism in the region of RS/BH is unique. It has provided both insights into the extension of the research fundus and improvement of ICT, social and new media usage, protection, and enablement for the RS/BH and global activist community. And with the redesigned Cyberactivist technical design and tool, a humble, but relevant contribution for the global activist community is made.

Bibliography

Aal, Konstantin, Weibert, Anne, Ahmadi, Michael, Rohde, Markus, Wulf, Volker. (2021). Soziale Medien in politischen Konfliktsituationen mit Fokus auf den arabischen Frühling. In: Reuter, C. (eds) Sicherheitskritische Mensch-Computer-Interaktion. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-658-32795-8_29

Aal, Konstantin; Yerousis, George; Schubert, Kai; Hornung; Dominik; Stickel, Oliver; and Wulf, Volker. (2014). Come_in@palestine: adapting a german computer club concept to a palestinian refugee camp. In Proceedings of the 5th ACM international conference on Collaboration across boundaries: culture, distance & technology (CABS '14). ACM, New York, NY, USA, 111-120. http://dx.doi.org/10.1145/2631488.2631498

Abu-Salma, Ruba; Krol, K.; Parkin, S.; Koh, V.; Kwan, K.; Mahboob, J.; Traboulsi, Z.; and Sasse, M. A. (2017). The security blanket of the chat world: An analytic evaluation and a user study of telegram. EuroUSEC.

Abu-Salma, Ruba; Sasse, M. A.; Bonneau, J.; Danilova, A.; Naiakshina, A.; & Smith, M. (2017). Obstacles to the adoption of secure communication tools. In: Security and Privacy (SP), 2017 IEEE Symposium on, pp. 137-153.

Abu-Tayeh, G.; Neumann, O.; and Stuermer, M. (2018). Exploring the motives of citizen reporting engagement: Self-concern and other-orientation. Business & information systems engineering, 60(3), pp. 215-226.

Academic Frontier Project. Survey on the Internet Security Awareness, http://www.kansai-u.ac.jp/riss/en/shareduse/data/17_E_questionnaire.pdf, last accessed 2017/06/17

Acar, Yasemin; Fahl, Sascha; Mazurek, Michelle L. (2016). You are not your developer, either: A research agenda for usable security and privacy research beyond end users. In: Cybersecurity Development (SecDev), IEEE, pp. 3-8.

Acquisti, Alessandro; and Gross, Ralph. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Lecture Notes in Computer Science book series LNCS, vol. 4258, pp. 36-58.

Adams, A. and Sasse, M.A. (1999). "Users Are Not the Enemy: Why Users Compromise Computer Security Mechanisms and How to Take Remedial Measures," Comm. ACM, vol. 42, Dec. 1999, pp. 40–46.

Agarwal, N.; Lim, M.; and Wigand, R. (2012). Raising and rising voices in social media. Business & Information Systems Engineering, 4(3), pp. 113-126.

Ahmed, Syed Ishtiaque; Haque, M.R.; Chen, J.; and Dell, N. (2017). Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. Proceedings of the ACM on Human-Computer Interaction, (CSCW), vol. 1, pp. 17.

Ahmed, Syed Ishtiaque; Haque, M.R.; Guha, S.; Rifat, M.R.; and Dell, N. (2017). Privacy, security, and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM. pp. 906-918.

Al Jazeera. (2019). "'Pravda za Davida i Dženana' u Beču: Idemo do kraja". https://balkans.aljazeera.net/vijesti/pravda-za-davida-i-dzenana-u-becu-idemo-do-kraja. Accessed 06 June 2019.

Al-Ani, Ban; Mark, Gloria; Chung, Justin; and Jones, Jennifer. (2012). The Egyptian blogosphere: a counter-narrative of the revolution. In Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work (CSCW '12). ACM, New York, NY, USA, pp. 17-26. http://dx.doi.org/10.1145/2145204.2145213

Alexander, Anne and Aouragh, Miriyam. (2014). Egypt's unfinished revolution: the role of the media revisited. *International Journal of Communication*, 8: 890-915.

Ali Bassam, Mahmoud; and Reisel, William D. (2015). "Exploring personal experience of wartime crisis effects on job insecurity in Syria." In *Psihologia Resurselor Umane,* vol. 13.2. pp. 245

Al-Jazeera (2021). Gaza-based journalists say their accounts blocked by WhatsApp. https://www.aljazeera.com/news/2021/5/25/israel-blocks-whatsapp-accounts-of-gaza-journalists. Accessed 30.12.2021

Almohamed Asam; and Vyas Dhaval. (2016). Designing for the Marginalized: A step towards understanding the lives of refugees and asylum seekers. In *Proceedings of the Conference Companion Publication on Designing Interactive Systems (DIS '16 Companion)*, pp. 165–168. http://doi.org/http://dx.doi.org/10.1145/2908805.290941

AlternativeTo - crowdsourced software recommendations. https://alternativeto.net. Accessed 11 July 2019.

Amazon. (2022). https://learnsecurity.amazon.com. Accessed 15.1.2022

Anderson, C., & Kirkpatrick, S. (2016). Narrative interviewing. International journal of clinical pharmacy, 38(3), pp. 631-634.

Armakolas, Ioannis and Maksimovic, Maja. (2013). *"Babylution": A Civic Awakening in Bosnia and Herzegovina?.* Eliamep Working Paper 34. Hellenic Foundation for European and Foreign Policy.

Asad, Mariam and Le Dantec, Christopher A. (2015). Illegitimate Civic Participation: Supporting Community Activists on the Ground. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15). ACM, New York, NY, USA, 1694-1703. http://dx.doi.org/10.1145/2675133.2675156

AwareEC. (2022). https://aware.eccouncil.org. Accessed 15.1.2022

Ayalon, Oshrat; Eran Toch; Irit Hadar; and Michael Birnhack. (2017). How Developers Make Design Decisions about Users' Privacy: The Place of Professional Communities and Organizational Climate. In Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, pp. 135-138.

Baek, Young Min; Kim, Eun-mee and Bae, Young. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. In Computers in Human Behavior, vol. 31, pp. 48-56. DOI: 10.1016/j.soscij.2014.07.002

BalkanInsight. (2020). https://balkaninsight.com/2020/06/18/castle-kako-srpska-vlast-manipulise-razumom-a-gradani-za-to-jos-i-placaju. Accessed 8.1.2022

Banjalukain. (2015). Zašto je zaista uhapšen Sanel Menzil iz Kotor Varoši: Sporni fotografija i komentar. Retrieved September 10, 2015 from http://banjalukain.com/clanak/130103/zasto-je-zaista-uhapsen-sanel-menzil-iz-kotor-varosi-sporni-fotografija-i-komentar

Barakovic, Vedava. (2011). Facebook Revolutions: The Case of Bosnia and Herzegovina. *Acta Universitatis Sapientiae. Social Analysis 1,2:* 194–205.

Barnard-Wills, David. (2013). Security, Privacy and Surveillance in European policy documents. In: International Data Privacy Law vol. 3, no. 3, pp. 170–180

Barth, Susanne; and De Jong, Menno DT. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics and Informatics, vol. 34, no. 7, pp. 1038-1058.

Bartsch, Miriam; and Dienlin, Tobias. (2016). Control your Facebook: An analysis of online privacy literacy. Computers in Human Behavior, vol. 56, pp. 147-154.

Batmanghelidj, Esfandyar. (2019). Bloomberg. Try As it Might, Iran Can't Ban Social Media, https://www.bloomberg.com/amp/opinion/articles/2019-01-10/iran-s-attempt-to-ban-instagram-is-doomed-to-fail. Accessed 8 May 2019.

Baum, Katharina; Meißner, Stefan; Abramova, Olga; and Krasnova, Hanna. (2019). Do they really care about targeted political ads? Investigation of user privacy concerns and preferences. In Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden, June 8-14, 2019. ISBN 978-1-7336325-0-8 Research Papers.

Bejtagić-Makić, Merima. (2013). Key drivers for customer engagement on Facebook brand fan pages in Bosnia and Herzegovina. In: International Conference on Economic and Social Studies, 10-11 May, Sarajevo. International Burch University.

Birge, C. (2009). Enhancing research into usable privacy and security. In Proceedings of the 27th ACM international conference on Design of communication, pp. 221-226.

Blackwell, Lindsay; Hardy, Jean; Ammari, Tawfiq; Veinot, Tiffany; Lampe, Cliff; and Sarita Schoenebeck. (2016). LGBT Parents and Social Media: Advocacy, Privacy, and Disclosure during Shifting Social Movements. In *Proceedings of the CHI'16*, San Jose, CA, USA, pp. 610-622.

BN TV. (2018). "Obračun vlasti sa grupom PzD". https://www.rtvbn.com/3926582/kako-je-dodik-i-najavio-obracun-vlasti-sa-aktivistima-pokreta-pravda-za-davida. Accessed 28 October 2018.

BN TV. Pravda za Davida: Poruka ubicama. http://www.rtvbn.com/3927142/pravda-za-davida-poruka-ubicama-. Accessed 28 October 2018.

Bonilla, Yarimar; and Rosa, Jonathan. (2015). # Ferguson: Digital protest, hashtag ethnography, and the racial politics of social media in the United States. American Ethnologist, vol. 42., no. 1, pp. 4-17. DOI: 10.1111/amet.12112

Borge-Holthoefer, Javier; Magdy, Walid; Darwish, Kareem; and Weber, Ingmar. (2015). "Content and network dynamics behind Egyptian political polarization on Twitter." In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing. ACM, pp. 700-711.

Borghoff, Uwe M., & Schlichter, Johann H. (2000). Computer-supported cooperative work. In Computer-supported cooperative work. Springer, Berlin, Heidelberg, pp. 87-141

Boulus-Rødje, Nina; and Bjørn Pernille. (2019). Digital (Occupied) Palestine. In *CHI2019 Workshop Proceedings - With an Eye to the Future: HCI Research and Practice in the Arab World*. March 2019, pp. 15 – 21. https://doi.org/10.1145/3290607.3299006

Bowles, Nellie. (2018). "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse, New York Times". https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html. Accessed 1 July 2018.

Boyd, D. Eric; Benjamin; McGarry Michael; and Clarke, Theresa B. (2016). Exploring the empowering and paradoxical relationship between social media and CSR activism. In Journal of Business Research, vol. 69, no. 8, pp. 2739–2746.

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares? First Monday, 15(8). https://doi.org/10.5210/fm.v15i8.3086

Bradshaw, Samantha; and Philip Howard. (2017). Troops, trolls and troublemakers: A global inventory of organized social media manipulation, Oxford Internet Institute, vol. 2017.12, pp. 1–37.

Brandtzeg, P. B.; Lüders, M.; and Skjetne, J. H. (2010). Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites. Intl. Journal of Human–Computer Interaction, 26(11-12), pp. 1006-1030.

Brennan, Michael; Metzroth, Katey; Stafford, Roxann. (2014). Building More Effective Internet Freedom Tools: Needfinding with the Tibetan Exile Community.

Brüsemeister, Thomas. (2008). *Qualitative Forschung*. Springer.

Bryan, Anabel. (2006). CSCW & Groupware Computer Supported Cooperative Work. https://slideplayer.com/slide/6617785. Accessed 30.12.2021

Buhl, H. U. (2011). From revolution to participation: Social media and the democratic decision-making process. DOI 10.1007/s12599-011-0166-4

Buka TV. (2021). https://www.youtube.com/watch?v=Qd7m3jF8NC8. Accessed 31.3.2022.

Buka. Facebook Group (>204000 members). Retrieved January 04, 2015 from https://facebook.com/bukamagazin

Buka. (2012). Retrieved January 04, 2013. http://6yka.com/novost/25133/tuca-izmedu-policije-i-setaca-ispred-zgrade-rtrs-a

Buka. (2022). Retrieved January 04, 2015 from https://6yka.com/bih/hakerski-napad-na-facebook-grupu-portala-buka

Burnore, Nathanael O. (2013). Social Media Applications for Unconventional Warfare. Faculty of the U.S. Army Command and General Staff College.

Business Monitor International. (2015). Telecommunications Report. Retrieved January 28, 2015 from http://marketresearch.com/Business-Monitor-International-v304/Bosnia-Herzegovina-Telecommunications-Q1-8516444

Caren, Neal; and Gaby, Sarah. (2011). Occupy Online: Facebook and the Spread of Occupy Wall Street. Social Science Reseach Network. Retrieved on June 15 2014 from http://dx.doi.org/10.2139/ssrn.1943168

Cavoukian, A. (2016). The 7 foundational principles: Implementation and mapping of fair information practices. https://gpsbydesign. org/the-7-foundational-princides-implementation-and-ma-pping-of-fair-information-practices. Accessed 19.1.2022

Cavoukian, Ann. (2009). Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada 5.

Centar za edukaciju Pro Educa Banja Luka. (2016). "Novinarstvo i drustvene mreze u BiH – Istrazivanje". http://proeduca.net/wp-content/uploads/2015/08/Novinarstvo-i-dru%C5%A1tvene-mre%C5%BEe-u-BiH-Istra%C5%BEivanje.pdf. Accessed 18 March 2018.

Centar za zivotnu sredinu. Facebook Group (>14000 members). Retrieved January 04, 2015 from https://www.facebook.com/CentarZaZivotnuSredinu

Chen, Hongliang; Beaudoin, Christopher E.; and Hong, Traci. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. Computers in Human Behavior, vol. 70, pp. 291-302.

Chen, Jay; Paik, Michael; and Mccabe, Kelly. (2014). Exploring Internet Security Perceptions and Practices in Urban Ghana. In SOUP, pp. 129-142.

Choudhary, Alok; Hendrix, W.; Lee, K.; Palsetia, D.; & Liao, W. K. (2012). Social media evolution of the Egyptian revolution. In *Communications of the ACM*, vol. 55(5), pp. 74-80.

Clifford, James; and Marcus, George E. (1986). Writing culture: The poetics and politics of ethnography. Univ of California Press.

Colakovic, Namik; and Markic, Marinko. (2010). Informacione i komunikacione tehnologije u funkciji zaštite okoliša. In *Univerzitetska Hronika* 5, University of Travnik, Travnik, B-H: 175-181.

Consumer Reports, Security Planer, https://securityplanner.consumerreports.org. Accessed 17 August 2021.

Cranor, Lorrie Faith; and Rebecca N. Wright. (2000). Influencing software usage. In Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions, pp. 45-55.

Cyentia. (2022). Iris Risk Retina Nonprofit, https://www.cyentia.com/wp-content/uploads/Cyentia-Retina-Nonprofit.pdf. Accessed 25.3.2022

Datareportal. (2021). https://datareportal.com/reports/digital-2021-bosnia-and-herzegovina. Accessed 8.1.2022

De Castro Leal, Debora; Krüger, M.; Misaki K.; Randall, D.; and Wulf, V. (2019). Guerilla Warfare and the Use of New (and Some Old) Technology: Lessons from FARC's Armed Struggle in Colombia. In *ACM Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems.* pp. 580.

Delegation of European Union to B-H. 2014. *Civil Society*. Retrieved February 28, 2015 from http://europa.ba/Default.aspx?id=33&lang=EN

Deutschland Sicher im Netz. (2017). „Sicherheitscheck“. https://www.dsin-sicherheitscheck.de. Accessed 15 June 2017.

Dewey, John and Rogers, Melvin. L. 2012. *The Public and Its Problems: An Essay in Political Inquiry.* Penn State University Press

DeWitt, A. J., & Kuljis, J. (2006). Aligning usability and security: a usability study of Polaris. In Proceedings of the second symposium on Usable privacy and security, pp. 1-7.

Dillet, Romain. (2021). Bodyguard is a mobile app that hides toxic content on social platforms. https://techcrunch.com/2021/01/21/bodyguard-is-a-mobile-app-that-hides-toxic-content-on-social-platforms. Accessed 30.12.2021

Dnevnik.ba. (2021). https://www.dnevnik.ba/teme/tko-se-protivi-pristupanju-bih-u-eu-i-zasto. Accessed 15.1.2022

Dourish Paul; Grinter, E.; Delgado De La Flor, J.; and Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. Personal Ubiquitous Computing. vol. 8, no. 6, pp. 391-401.

Dourish, Paul. (2010). CHI and environmental sustainability: the politics of design and the design of politics. In: Proceedings of the 8th ACM conference on designing interactive systems, pp. 1–10. http://doi.org/10.1145/1858171.1858173

Drake JR; Hall D; Becton JB; Posey C (2016) Job applicants' information privacy protection responses: Using social media for candidate screening. In: AIS Transactions on Human Computer Interaction, Volume 8, Issue 4, pp 160-184

Drljaca, Dalibor; and Latinovic, Branko. (2017). Social Networks As Tool For E-Government–Case Study Of Republic Of Srpska Government. Metteg14. pp. 41.

DSIN. (2021). https://www.dsin-sicherheitscheck.de. Accessed 30.12.2021

Eacea. (2021). https://eacea.ec.europa.eu/national-policies/eurydice/bosnia-and-herzegovina/population-demographic-situation-languages-and-religions_cs. Accessed 16.1.2022

Egelman, S., King, J., Miller, R. C., Ragouzis, N., & Shehan, E. (2007, April). Security user studies: methodologies and best practices. In CHI'07 extended abstracts on Human factors in computing systems, pp. 2833-2836.

Egelman, Serge; and Eyal Peer. (2015). The myth of the average user: Improving privacy and security systems through individualization. In Proceedings of the 2015 New Security Paradigms Workshop, pp. 16-28.

Ehrlinger, J.; Gilovich, T.; and Ross, L. (2004). Peering Into the Bias Blind Spot: People“s Assessments of Bias in Themselves and Others. Personality and Social Psychology Bulletin 31(5), pp. 680-692.

E-trafika. Facebook Group (>10700 members). Retrieved January 04, 2015 from https://facebook.com/etrafika

Etter, Lauren. (2017). Bloomberg. What happens when the government uses Facebook as a weapon? https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook. Retrieved 9 December 2017.

EU Commission. (2019). Analytical Report accompanying the document Communication from the Commission to the European Parliament and the Council Commission Opinion on Bosnia and Herzegovina's application for membership of the European Union. https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-bosnia-and-herzegovina-analytical-report.pdf. Accessed 10 June 2019.

EUReportBH. (2021). https://ec.europa.eu/neighbourhood-enlargement/bosnia-and-herzegovina-report-2021_en. Accessed 12.1.2022

Europa.ba. (2019). "EU Delegation/EUSR in BH deeply concerned with situation in Banja Luka and call for calm". http://europa.ba/?p=61402. Accessed 02 February 2019.

Europa.ba. (2021). https://europa.ba/?page_id=484. Accessed 15.1.2022

European Commission. (2016). "Bosnia and Herzegovina 2016 Report". https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2016/ 20161109_report_bosnia_and_herzegovina.pdf. Accessed 14 April 2018.

European Commission. (2014). Key findings of the Progress Report on Bosnia and Herzegovina. Retrieved February 28, 2015 from http://ec.europa.eu/ enlargement/pdf/key_documents/2014/20141008-bosnia-and-herzegovina-progress-report_en.pdf

Federal Trade Commission. (2017). "Privacy impact assessments". https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments. Accessed 17 June 2017.

Ferwerda, Bruce, Chen, Lee, & Tkalcic, Marko. (2021). Research Topic Psychological Models for Personalized Human-Computer Interaction (HCI). Frontiers in psychology, 12, 1025.

Foth, Marcus; Tomitsch, Martin; Satchell, Christine; and Haeusler, M. Hank. (2015). From users to citizens: Some thoughts on designing for polity and civics. In Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction. ACM, pp. 623-633.

FreeEurope. (2015). https://www.slobodnaevropa.org/a/kako-djeluju-crnogorski-stranacki-botovi/26947313.html. Accessed 8.1.2022

Freelon, D., Lynch, M., & Aday, S. (2015). Online fragmentation in wartime: A longitudinal analysis of tweets about Syria, 2011–2013. The ANNALS of the American Academy of Political and Social Science, 659(1), 166-179.

Friedewald, Michael; Van Lieshout, Marc; and Rung, Sven. (2016). Privacy and Identity Management, Springer.

Friedewald, Michael; Van Lieshout, Marc; and Sven Rung. (2015). Modelling the Relationship Between Privacy and Security Perceptions and the Acceptance of Surveillance Practices, In: IFIP International Summer School on Privacy and Identity Management, pp. 1-18.

Friedewald, Michael; Van Lieshout, Marc; Rung, Sven; and Oom, Merel. (2016). The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security. Law, Governance and Technology Series, vol. 24, pp. 51-74. DOI: 10.1007/978-94-017-7376-8_3

Friedrich Ebert Stiftung B-H. Facebook Group (>820 members). Retrieved January 04, 2015 from https://facebook.com/FESBiH

Frik, Alisa; Leysan Nurgalieva; Bernd, Julia; Lee, Joyce; Schaub, Florian; and Serge Egelman. (2019). Privacy and security threat models and mitigation strategies of older adults. In Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019).

Fullam J (2017) Becoming a youth activist in the internet age: a case study on social media activism and identity development. In: International Journal of Qualitative Studies in Education Vol. 30, Issue 4, pp 406-422. doi: 10.1080/09518398.2016.1250176.

Gahagan, Kassandra; Vaterlaus, Jay Mitchell; and Frost, Libby R. (2016). College student cyberbullying on social networking sites: Conceptualization, prevalence, and perceived bystander responsibility. In Computers in human behavior, vol. 55, pp. 1097-1105. https://doi.org/10.1016/j.chb.2015.11.019

Gao, Huiji; Barbier, Geoffrey; Goolsby, Rebecca; and Zeng, Daniel. (2011). Harnessing the crowdsourcing power of social media for disaster relief. Arizona State Univ Tempe.

Gaw, Shirley; Edward W. Felten; and Patricia Fernandez-Kelly. (2006). Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In: Proceedings of the SIGCHI conference on human factors in computing systems. ACM, pp. 591-600.

Gee, James Paul. (2014). *An Introduction to Discourse Analysis: Theory and Method* (4th. ed.). Routledge.

Geertz, Clifford. (1973). The interpretation of cultures. Vol. 5043. Basic books.

Geiger, Stuart R.; and Ribes, David. (2011). Trace ethnography: Following coordination through documentary practices. In System Sciences (HICSS), 44th Hawaii International Conference on, pp. 1-10.

Geismann, J., Gerking, C., & Bodden, E. (2018). Towards ensuring security by design in cyber-physical systems engineering processes. In Proceedings of the 2018 International Conference on Software and System Process (pp. 123-127).

General Framework Agreement for Peace in Bosnia & Herzegovina. (1995). Retrieved December 28, 2015 from http://peacemaker.un.org/sites/peacemaker.un.org/files/BA_951121_DaytonAgreement.pdf

Gerbaudo, Paolo. (2018). Tweets and the streets: Social media and contemporary activism. Pluto Press.

Giacaman, Rita; Husseini, Abdullatif; Gordon, N. H.; and Awartani, F. (2004). Imprints on the consciousness: the impact on Palestinian civilians of the Israeli army invasion of West Bank towns. In *The European Journal of Public Health*, vol. 14(3), pp. 286-290.

Gilovich, Thomas (1991). How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life. New York: Free Press.

Goecks, Jeremy, Voida, Amy, Voida, Stephen, and Mynatt, Elizabeth D.. (2008). Charitable technologies: opportunities for collaborative computing in non-profit fundraising. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work* (CSCW '08). ACM, New York, NY, USA, 689-698. http://dx.doi.org/10.1145/1460563.1460669

Goel, Vindu; and Rahman, Shaikh Azizur. (2019). New York Times. When Rohingya Refugees Fled to India, Hate on Facebook Followed. https://www.nytimes.com/2019/06/14/technology/ facebook-hate-speech-rohingya-india.html. Accessed 10 July 2019.

Grazia. Let's Face It: We Could All Do With A Social Media Curfew. https://graziadaily.co.uk/life/in-the-news/social-media-curfew. Accessed 21 April 2019.

Gritzalis D; Kandias M; Stavrou V; Mitrou L (2014). History of Information: The case of Privacy and Security in Social Media. In: Proc. of the History of Information Conference pp. 283-310, Athens, Greece

Gross, Joshua B.; and Mary Beth Rosson. (2007a). End user concern about security and privacy threats. In Proceedings of the 3rd symposium on Usable privacy and security, pp. 167-168.

Gross, Joshua B.; and Mary Beth Rosson. (2007b). Looking for trouble: understanding end-user security management. In Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology, pp. 10-es.

Grubbs Hoy, Mariea and Phelps, Joseph. (2008). Online privacy and security practices of the 100 largest US non-profit organizations. In *International Journal of Nonprofit and Voluntary Sector Marketing*, 14, 1: 71–82. http://dx.doi.org/10.1002/nvsm.344

Gurstein, Michael. (1999). *Community Informatics: Enabling Communities with Information and Communications Technologies.* Idea Group Publishing.

Gyöngy, Antonela. (2019). New media used in the context of the Syrian conflict. In *Review of the Air Force Academy*, no.1, vol. 39. DOI: 10.19062/1842-9238.2019.17.1.6

Hacker, Janine; Riemer, Kai. (2021). Identification of user roles in enterprise social networks: method development and application. Business & Information Systems Engineering, 63(4), 367-387.

Hardaker, Claire. (2010). Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions. *Journal of Politeness Research* 6: 215-242. http://dx.doi.org/10.1515/JPLR.2010.011

Harlow, Summer. (2012). Social media and social movements: Facebook and an online Guatemalan justice movement that moved offline. In: New Media & Society, vol. 14, issue 2, pp. 225-243. DOI: 10.1177/1461444811410408

Hazazi, Hussein. (2017). 150 Saudis are preparing in the "Peace Army" to repel hostile cyber attacks. https://www.okaz.com.sa/article/1553356. Accessed 28 June 2019.

Hegelich, Simon. (2015). Social Botnets als politische Meinungsmacher in der Ukraine: Big-Data-Methoden zur Analyse von Twitter-Manipulationen. Retrieved April 20th, 2015 from http://www.rundfunk-institut.uni-koeln.de/sites/rundfunk/Tagungen/ Tagung2015/Hegelich.pdf

Helfferich, Cornelia. (2009). Die Qualität qualitativer Daten - Manual für die Durchführung qualitativer Interviews (4th ed.). Verlag für Sozialwissenschaften, Wiesbaden, Germany.

Hellman, J., Cheng, J., & Guo, J. L. (2021). Facilitating Asynchronous Participatory Design of Open Source Software: Bringing End Users into the Loop. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, pp. 1-7.

Helsinski parlament gradjana. Facebook Group (>1300 members). Retrieved January 04, 2015 from https://facebook.com/pages/ Helsin%C5%A1ki-parlament-gra%C4%91ana-Banja-Luka/1425435307682325

Herley, Cormack. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. In Proceedings of the 2009 New Security Paradigms Workshop, NSPW '09, New York, NY, USA, ACM, pp. 133-144.

Herzog, Almut; and Nahid Shahmehri. (2007). User help techniques for usable security. In Proceedings of the 2007 symposium on Computer human interaction for the management of information technology, pp. 11-es.

Hocemo JMBG za nasu djecu. Facebook Group (>1740 members). Retrieved January 04, 2015 from https://facebook.com/groups/ 592849114079390

Howard, Philip N. 2011. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam.* Oxford University Press

Howard, Philip N.; Duffy, Aiden; Freelon, Deen; Hussain, M. M.; Mari, Will; and Maziad, M. (2011). Opening closed regimes: what was the role of social media during the Arab Spring?. Available at SSRN 2595096.

IDEA.INT. (2019). "Voter turnout BH". https://www.idea.int/data-tools/data/voter-turnout. Accessed 08 February 2019.

Information Security Awareness Questionnaire, Warwick University. http://warwick.ac.uk/services/gov/informationsecurity/questionnaire. Accessed 17 June 2017.

International Computer Science Institute. (2022). Privacy Group. https://www.icsi.berkeley.edu/icsi/groups/privacy. Accessed 17.1.2022.

Internet Privacy Practices, Self-assessment, https://libraryfreedomproject.org/wp-content/uploads/2016/02/privacy-assessment-tool-to-print.pdf, last accessed 2017/06/17

Internet World Stats. (2021). https://www.internetworldstats.com/europa2.htm#ba. Accessed 18 July 2021.

Internet World Stats. (2015). Retrieved February 28, 2015 from http://internetworldstats.com/stats4.htm

IRB. (2022). https://www.irbrs.net/statistika/UporedniPrikaz.aspx?tab=3&lang=lat. Accessed 3.4.2022

Jakobi, Timo; von Grafenstein, M.; Legner, C.; Labadie, C.; Mertens, P.; Öksüz, A.; and Stevens, G. (2020). The Role of IS in the Conflicting Interests Regarding GDPR. Business & Information Systems Engineering, pp. 1-12.

Johnson, Lakitta D.; Haralson, Alfonso; Batts, Sierra; Brown, Ebonie; Collins, Cedric; Van Buren-Travis, Adrian; and Spencer, Melissa. (2016). Cyberbullying on Social Media Among College Students. In Ideas and Research You Can Use: VISTAS 2016.

Jonjic, Andrea. (2014). Auf Lethargie folgt Revolution? Die Proteste in Bosnien und Herzegowina. Retrieved on March 3, 2014 from http://sicherheitspolitik-blog.de/2014/03/03/auf-lethargie-folgt-revolution-die-proteste-in-bosnien-und-herzegowina

Jordaan, Yolanda; and Van Heerden, Gene. (2017). Online privacy-related predictors of Facebook usage intensity. In Computers in Human Behavior, vol. 70, pp. 90-96.

Juris, Jeffrey S. (2012). Reflections on #Occupy Everywhere: Social media, public space, and emerging logics of aggregation. In *American Ethnologist 39*: 259–279. http://dx.doi.org/10.1111/j.1548-1425.2012.01362.x

Kahneman, Daniel; and Dan Lovallo. (1993). Timid choices and bold forecasts: A cognitive perspective on risk taking. Management science 39, no. 1, pp 17-31.

Kallas P, Top 15 Most Popular Social Networking Sites and Apps, https://www.dreamgrow.com/top-15-most-popular-social-networking-sites, last accessed 2018/01/28

Kar B; Ghose R (2014) Is My Information Private? Geo-Privacy in the World of Social Media. In: GIO@ GIScience, pp 28-31

Karganovic, Stefan. (2014). Kako se priprema puc - tehnologija obojenih revolucija. In *Rusenje Republike Srpske -Teorija i tehnologija prevrata,* Stefan Karganovic, Pjotr Iljcenkov, John Lockland, Irina Lebedeva, Johnatan Movat and Nebojsa Malic. Besjeda, Banja Luka, B-H, 14-15.

Kazansky B (2015) Privacy, Responsibility, and Human Rights Activism. In: FCJ-195, The Fibreculture Journal, Issue 26

Khamis, Sahar and Vaughn, Katherine. (2011). Cyberactivism in the Egyptian Revolution: How Civic Engagement and Citizen Journalism. In *Arab Media and Society* 14, 3: 1-25.

Khodabakhshi, Leyla. (2018). "Why ordinary Iranians are turning to internet backdoors to beat censorship". https://www.bbc.com/news/blogs-trending-42612546. Accessed 02 November 2021.

Khondker, Habibul Haque. (2011). Role of the New Media in the Arab Spring. In *Globalizations* 8. 5: 675-679. http://dx.doi.org/10.1080/14747731.2011.621287

Klausen, Jytte. (2015). Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq. In *Studies in Conflict & Terrorism*. Vol. 38.1. pp. 1-22.

Klix.ba. (2019). "Koji kandidati za predsjednistvo BiH Facebook koriste za komunikaciju s gradjanima". https://www.klix.ba/vijesti/bih/koji-kandidati-za-predsjednistvo-bih-facebook-koriste-za-komunikaciju-s-gradjanima/180923100. Accessed 08 February 2019.

Klix.ba. (2018). SIPA vrsi provjere zbog poruka Rajka Vasica na Twitteru: uklonjen tweet u kojem je prijetio genocidom. https://www.klix.ba/vijesti/bih/sipa-vrsi-provjere-zbog-poruka-rajka-vasica-na-twitteru-uklonjen-tweet-u-kojem-je-prijetio-genocidom/180713128. Accessed 13 July 2018.

Koruga, Petra; and Baca, Miroslav. (2012). Communication of political parties on Twitter: Comparison of political parties in Serbia, Croatia, Slovenia and BiH. In: XIII International Symposium SYMORG.

Kou, Yubo; and Nardi, Bonnie. (2018). Complex Mediation in the Formation of Political Opinions. 10.1145/3173574.3174210.

Kow, Yong Ming; Kou, Yubo; Semaan, Bryan; and Cheng, Waikuen. (2016). Mediating the undercurrents: Using social media to sustain a social movement. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. ACM, pp. 3883-3894.

Kremic, Tibor; Tukel, Oya Icmeli; and Rom, Walter O. 2006. Outsourcing decision support: a survey of benefits, risks, and decision factors. *Supply Chain Management: An International Journal* 11, 6: 467 – 482. http://dx.doi.org/10.1108/13598540610703864

Krippendorff, Klaus. 2004. *Content Analysis: An Introduction to Its Methodology.* Thousand Oaks. Sage Publications Inc.

Kumaraguru P. Privacy and Security in Online Social Networks, NOC, https://onlinecourses.nptel.ac.in/noc16_cs07/preview, last accessed 2017/06/17

Kuntsman, Adi; and Rebecca L. Stein. (2015). *Digital militarism: Israel's occupation in the social media age.* Stanford University Press.

Kurtovic, Larisa. (2013). "Nationalist order and party patronage in post-Dayton BH". Scholar Research Brief, IREX/DePaul University, US. https://irex.org/resource/nationalist-order-and-party-patronage-post-dayton-bosnia-herzegovina-research-brief. Accessed 17 September 2014.

Küsters, I. (2009). Narrative Interviews: Grundlagen und Anwendungen. Springer-Verlag.

Küsters, Ivonne. (2006). Das narrative Interview im Forschungsprozess. In Narrative Interviews. Verlag für Sozialwissenschaften, Wiesbaden, Germany, pp. 39-176.

Kvale, S., & Brinkmann, S. (2009). Interviews: Learning the craft of qualitative research interviewing. Sage.

Lamnek, S., & Krell, C. (2005). Qualitative Sozialforschung. München: Psychologie Verlags Union.

Landwehr, Marvin; Borning, Alan; and Wulf, Volker. (2019). The High Cost of Free Services: Problems with Surveillance Capitalism and Possible Alternatives for IT Infrastructure. In *LIMITS'19*, June 10–11, 2019, Lappeenranta, Finland. https://doi.org/10.1145/3338103.3338106.

Lange-Ionatamishvili, E., Svetoka, S., & Geers, K. (2015). Strategic communications and social media in the Russia Ukraine conflict. Cyber War in Perspective: Russian Aggression against Ukraine, pp. 103-111.

Langer, Amanda; Kaufhold, Marc-André; Runft, Elena Maria; Reuter, Christian; Grinko, Margarita; and Pipek, Volkmar. (2019). Counter Narratives in Social Media–An Empirical Study on Combat and Prevention of Terrorism. In *Proceedings of the 16th ISCRAM Conference* – València, Spain, May 2019. pp. 746-755.

Langheinrich, Marc. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. In International conference on Ubiquitous Computing, pp. 273-291. Springer, Berlin, Heidelberg.

Latonero, Mark; and Shklovski, Irina. (2011). Emergency management, Twitter, and social media evangelism. In International Journal of Information Systems for Crisis Response and Management (IJISCRAM), vol. 3, no. 4, pp. 196-212. https://doi.org/10.4018/jiscrm.2011100101

Le Dantec, Christopher A.; and Edwards, W. Keith. (2010). Across boundaries of influence and accountability: the multiple scales of public sector information systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 113-122. http://dx.doi.org/10.1145/1753326.1753345

Levine, Timothy R.; Rachel K. Kim; Hee Sun Park; and Mikayla Hughes. (2006). Deception detection accuracy is a predictable linear function of message veracity base-rate: A formal test of Park and Levine's probability model. Communication Monographs 73, no. 3, pp. 243-260.

Likmeta, Besar. (2012). http://www.balkaninsight.com/en/article/activists-rally-against-road-expansion-in-tirana-park. Accessed 08.1.2022

Lim, Merlyna. (2012). Clicks, cabs, and coffee houses: Social media and oppositional movements in Egypt, 2004–2011. In *Journal of communication*, vol. 62.2, pp. 231-248.

Lipford, Heather Richter: Usable security: history, themes, and challenges. San Rafael, California, ISBN 978-1-62705-530-7.

Longhurst, R. (2003). Semi-structured interviews and focus groups. Key methods in geography, 3(2), pp. 143-156.

Lopreite, M., Panzarasa, P., Puliga, M., & Riccaboni, M. (2021). Early warnings of COVID-19 outbreaks across Europe from social media. Scientific reports, 11(1), pp. 1-7.

Lovejoy, Kristen; and Saxton, Gregory D. (2012). Information, Community, and Action: How Nonprofit Organizations Use Social Media. *Journal of Computer-Mediated Communication* 17, 3: 337-353. http://dx.doi.org/10.1111/j.1083-6101.2012.01576.x

Lovejoy, Kristen; Waters, Richard D.; and Saxton, Gregory D. (2012). Engaging stakeholders through Twitter: How non-profit organizations are getting more out of 140 characters or less. *PR Review* 38, 2: 313–318. http://dx.doi.org/10.1016/j.pubrev.2012.01.005

LucySecurity. (2022). https://lucysecurity.com. Accessed 15.1.2022

Ludwig, T., Stickel, O., Tolmie, P., & Sellmer, M. (2021). shARe-IT: Ad hoc Remote Troubleshooting through Augmented Reality. Computer Supported Cooperative Work (CSCW), 30(1), pp. 119-167.

Luo W; Xie Q; Hengartner U (2009) Facecloak: An architecture for user privacy on social networking sites. In: Computational Science and Engineering, 2009. CSE '09. International Conference on Computational Science and Engineering. IEEE. doi: 10.1109/CSE.2009.387

Lynch E. (2017) The New Social Imaginary vs. the Education Activist: Social Media as a Conduit for Protest and Resistance, Hofstra University

Lynch, Marc; Freelon, Dean; and Aday, Sean. (2016). How Social Media Undermines Transitions to Democracy. Blogs and Bullets IV: Peace Tech Lab

Madden M, Privacy management on social media sites, http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites, last accessed 2017/06/17

Madden M; Lenhart A; Cortesi S; Gasser U; Duggan M; Smith A; Beaton M (2013) Teens, social media, and privacy. Pew Research Center, 21 Jg, pp 2-86

Magolis D; Briggs A (2016) A Phenomenological Investigation of Social Networking Site Privacy Awareness through a Media Literacy Lens. In: Journal of Media Literacy Education, 8(2), pp 22 -34

Maitland, Carleen; Tomaszewski, Brian; and Karen E. Fisher. (2015). *Youth Mobile Phone and Internet Use, January 2015, Za'atari Camp, Mafraq, Jordan*. Penn State College of Information Sciences and Technology, vol. 19.

Malisic, Aleksandra. (2016). Provela sam nekoliko dana sa botovima i saznala da ne rade za sendviče. VICE. https://www.vice.com/rs/article/qk8755/provela-sam-nekoliko-dana-sa-botovima-i-saznala-da-ne-rade-za-sendvice. Accessed 28 November 2018.

Mark, Gloria; and Semaan, Bryan. (2008). Resilience in collaboration: Technology as a resource for new patterns of action. In: *Proceedings of the 2008 ACM conference on Computer supported cooperative work*, ACM, pp. 137-146.

Marreiros, Helia; Tonin, Mirco; and Vlassopoulos, Michael. (2016). 'Now that You Mention It': A Survey Experiment on Information, Salience and Online Privacy. In Journal of Economic Behavior & Organization, Vol 140, August 2016. pp. 1-17. https://doi.org/10.1016/j.jebo.2017.03.024

Martus. Benetech. https://www.martus.org. Accessed 17 August 2021.

Marwick, Alice E. (2012). The public domain: Social surveillance in everyday life. In: Surveillance & Society, vol. 9, no. 4, pp. 378.

Marzouki, Yousri; Skandrani-Marzouki, Inès; Béjaoui, Moez; Hammoudi, Haythem; and Bellaj, Tarek. (2012). The Contribution of Facebook to the 2011 Tunisian Revolution: A Cyberpsychological Insight. *Cyberpsychology, Behavior, and Social Networking*: 237-244. http://dx.doi.org/10.1089/cyber.2011.0177.

Masic, Izet; Sivic, Suad; and Pandza, Haris. (2012). Social networks in medical education in Bosnia and Herzegovina. Materia socio-medica, vol. 24, no. 3, pp. 162.

Massung, Elaine; Coyle, David; Cater, Kirsten F.; Jay, Marc; and Priest, Chris. (2013). Using crowdsourcing to support pro-environmental community activism. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13). ACM, New York, NY, USA, 371-380. http://dx.doi.org/10.1145/2470654.2470708

Mayring, Philipp. (2000). Qualitative Content Analysis. Retrieved June 05, 2014 from http://qualitative-research.net/index.php/fqs/article/view/1089

McCarthy, John; and Wright, Peter. (2015). Taking [A]part: The Politics and Aesthetics of Participation in Experience-Centered Design. MIT Press.

McGregor, Susan E.; Roesner, Franziska; and Caine, Kelly. (2016). Individual versus Organizational Computer Security and Privacy Concerns in Journalism. In Proceedings on Privacy Enhancing Technologies, 2016 (4), pp. 418–435.

McGregor, Susan E.; Watkins, E. A.; Al-Ameen, M. N.; Caine, K.; and Roesner, F. (2017). When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers. In Proceedings of the 27th Usenix Symposium, Vancouver, Canada.

McPhail, Brenda; Costantino, Terry; Bruckmann; David, Barclay, Ross; and Clement, Andrew. (1998). Caveat Exemplar: Participatory Design in a Non-Profit Volunteer Organisation. *Computer Supported Cooperative Work* 7, 3-4: 223-241. http://dx.doi.org/10.1023/A:3A1008631020266

Meikle, G. (2014). Social media, visibility and activism: the "Kony 2012" campaign. in: Ratto, M. and Boler, M. (ed.) DIY citizenship: critical making and social media Cambridge, Massachusetts MIT Press. pp. 373-384

Meis, M. (2017). When is a conflict a crisis? On the aesthetics of the Syrian civil war in a social media context. In: *Media, War & Conflict*, vol. 10, no. 1, pp. 69-86.

Meredith, Kristen. (2013). Social Media and Cyber Utopianism: Civil Society versus the Russian State during the 'White Revolution' 2011-2012. *St Antony's International Review 8, 2: 89-105.*

Merhul, Srivastava. (2016). Financial Times. How Erdogan turned to social media to help foil coup in Turkey. https://www.ft.com/content/3ab2a66c-4b59-11e6-88c5-db83e98a590a. Accessed 10 December 2017.

Milmo, Dan. (2022). The Guardian. Russia blocks access to Facebook and Twitter. https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter. Accessed 27.3.2022.

Moja Banjaluka. Agencija za zaštitu ličnih podataka u BiH pokrenula postupak protiv MUP RS. http://www.mojabanjaluka.info/single/47993. Accessed 11 July 2018.

Monroy-Hernández, Andrés; Boyd, Danah; Kiciman, Emre; De Choudhury, Munmun; and Counts, Scott. 2013. The new war correspondents: the rise of civic media curation in urban warfare. In*Proceedings of the 2013 conference on Computer supported cooperative work* (CSCW '13). ACM, New York, NY, USA, 1443-1452. http://dx.doi.org/10.1145/2441776.2441938

Morozov E (2011) The net delusion: The dark side of Internet freedom. Public Affairs, New York, USA

Morton, A., & Sasse, M. A. (2012). Privacy is a process, not a PET: A theory for effective privacy practice. In Proceedings of the 2012 New Security Paradigms Workshop, pp. 87-104.

Mosco, Vincent. (2019). Social media versus journalism and democracy. In Journalism, 20(1), pp. 181-184.

Mujkić, A. (2016). Bosnian Days of Reckoning: Review of the Sequence of Protests in Bosnia and Herzegovina 2013–14, and Future Prospects of Resistance, Southeastern Europe, 40(2), 217-242. doi: https://doi.org/10.1163/18763332-04002004

Mundt, M., Ross, K., & Burnett, C. M. (2018). Scaling social movements through social media: The case of Black Lives Matter. Social Media+ Society, 4(4), 2056305118807911.

Mylonas, Alexios; Kastania, Anastasia; and Gritzalis, Dimitris. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. Computer Security, vol. 34, pp. 47-66. DOI=http://dx.doi.org/10.1016/j.cose.2012.11.004

N1. (2018). "Čelnici MUP-a Republike Srpske tužili oca Davida Dragičevića". http://rs.n1info.com/a394601/Svet/Region/Celnici-MUP-a-Republike-Srpske-tuzili-oca-Davida-Dragicevica.html. Accessed 28 October 2018.

N1. (2020). "Perduv: Želimo srušiti režim u RS-u". http://ba.n1info.com/Vijesti/a411789/Pokret-pravde-zeli-da-srusi-rezim-u-RS.html. Accessed 21 March 2020

Naeini, Pardis Emami; Bhagavatula, Sruti; Habib, Hana; Degeling, Martin; Bauer, Lujo; Cranor, Lorrie Faith; and Sadeh, Norman. (2017). Privacy expectations and preferences in an IoT world. In Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017), pp. 399-412.

Nah, Seungahn; and Saxton, Gregory D. (2013). Modeling the adoption and use of social media by non-profit organizations, In *New Media & Society,* 15, 2: 294-313 http://dx.doi.org/10.1177/1461444812452411

Napoli, Daniela. (2018). Developing Accessible and Usable Security (ACCUS) Heuristics. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, pp. 1-6.

Net.hr. (2021). https://net.hr/danas/hrvatska/kakav-fail-hdz-ovci-kupili-botove-iz-egzoticnih-zemalja-da-im-udaraju-lajkove-na-fejs-postove-a-ovi-okidaju-iskljucivo-ljutka-4907a390-b1c8-11eb-9c2a-0242ac140035. Accessed 08.1.2022

Nezavisne Novine. (2018). Bijeljinac uhapšen zbog sumnje da je pozivao na napad na policiju. https://www.nezavisne.com/novosti/hronika/Mladic-iz-Bijeljine-uhapsen-zbog-sumnje-da-je-pozivao-na-napad-na-policiju/487113. Accessed 08 July 2018.

Niksirat, Kavous Salehzadeh; Anthoine-Milhomme, Evanne; Randin, Samuel; Huguenin Kévin and Cherubini, Mauro. "I thought you were okay": Participatory Design with Young Adults to Fight Multiparty Privacy Conflicts in Online Social Networks. Designing Interactive Systems Conference (DIS), ACM, Jun 2021, USA.

NN/UN. (2010). The Division for Social Policy and Development (DSPD) is part of the Department of Economic and Social Affairs (DESA) of the United Nations Secretariat. 2010. Why are ICTs important for Civil Society Organizations? Retrieved from Januar 6th, 2016 from http://www.un.org/esa/socdev/ngo/docs/2010/directory/ictcso.pdf

NSO Group. (2021). Transparency and Responsibility Report. https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf. Accessed 30.12.2021

ObscuraCam. Project Guardian. https://guardianproject.info/apps/obscuracam. Accessed 17 August 2021.

Occupy Banjaluka. Facebook Group (>770 members). Retrieved January 04, 2015 from https://facebook.com/groups/255985807771350

Online Privacy and Security Questionnaire, http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/questions/privacy.html, last accessed 2017/06/17

Panic Button. The Engine Room Blog. https://www.theengineroom.org/panic-button-retiring-the-app. Accessed 17 August 2021.

Park je nas. Facebook Group (>38400 members, ~15000 members in first 24 hours after group start). Retrieved January 04, 2015 from https://facebook.com/groups/park.je.nas

Pearce, Katy E.; and Kandzior, Sarah. (2012). Networked authoritarianism and social media in Azerbaijan. In *Journal of Communication*, vol. 62, no. 2, pp. 283-298.

Petkos G; Papadopoulos S (2015) PScore: A framework for enhancing privacy awareness in online social networks. In: Availability, Reliability and Security (ARES), 2015 10th International Conference on. IEEE, pp 592-600

Pickl, S. (2019). Interview with Erich Vad on "Political and Security Aspects of Digitization". Business & Information Systems Engineering, 61(3), pp. 257-260.

Poplave u regionu. Facebook Group (>49000 members). Retrieved September 20, 2015 from https://www.facebook.com/Poplave-u-regionu-1441672986080458

Pravda za Davida, Facebook group. (2018). https://www.facebook.com/groups/PravdaZaDavida. Accessed 27 October 2018.

Prinz, Wolfgang. (2018). Blockchain and CSCW–Shall we care?. In *Poceedings of 16th European Conference on Computer-Supported Cooperative Work-Exploratory Papers*. European Society for Socially Embedded Technologies (EUSSET)

Privacy manager - Bewerte deine Facebook-Einstellungen. http://www.privacy-manager.net. Accessed 18 July 2019.

Privacy tools. https://www.privacytools.io. Accessed 02 February 2019.

Project Shield. Jigsaw. https://projectshield.withgoogle.com. Accessed 18 March 2019.

Project Tor. https://www.torproject.org. Accessed 17 August 2021.

Purdue University, Information Security Questionnaire, https://www.cerias.purdue.edu/assets/pdf/k-12/questionnaire/infosec_questionnaire.pdf, last accessed 2017/06/17

Radio Sarajevo. (2018). Društvene mreže / Bh. institucije kaskaju za svjetskim tokovima. https://www.radiosarajevo.ba/vijesti/bosna-i-hercegovina/bh-institucije-i-drustvene-mreze-samo-rijetki-koriste-facebook-i-twitter/262656. Accessed 18 March 2018.

Rancière, Jacques (2015). Dissensus: On politics and aesthetics. Bloomsbury Publishing

Randall, David; Harper, Richard; and Rouncefield, Mark. (2007). Fieldwork for design: theory and practice. Springer Science & Business Media.

Rathi, Dinesh; Given, Lisa; Forcier, Eric; and Vela, Sarah. (2014). Every Task its Tool, Every Tool its Task: Social Media Use in Canadian Non-Profit Organizations. In *Proceedings of the CAIS.* Retrieved April 5, 2015 from http://www. cais-acsi.ca/ojs/index.php/cais/article/view/90

Reichertz, Jo. (2009). Abduction: The Logic of Discovery of Grounded Theory. *Forum Qualitative Social Research*, vol. 11, no. 1. ISSN 1438-5627. pp. 1. doi:http://dx.doi.org/10.17169/fqs-11.1.1412

Reljic, Dusan. (2004). The News Media and the Transformation of Ethnopolitical Conflicts. In *Transforming Ethnopolitical Conflict*, Austin A., Fischer, M., Ropers, N. Verlag für Sozialwissenschaften, Wiesbaden, DE, 321-339. http://dx.doi.org/10.1007/978-3-663-05642-3_16

Republika Srpska Ministry of Internal Affairs. (2015). Announcement. Retrieved January 27, 2015 from http://mup.vladars.net/lat/index.php?vijest=11693&vrsta=saopstenja

Reuter, C.; Hughes, A. L.; and Kaufhold, M. A. (2018). Social media in crisis management: An evaluation and analysis of crisis informatics research. International Journal of Human–Computer Interaction, 34(4), pp. 280-294.

Reuters. (2022). https://www.reuters.com/markets/commodities/serbia-may-suspend-lithium-deal-with-rio-tinto-pm-brnabic-2022-01-08. Accessed 30.12.2021

Ring, Edan. (2021). London Review of Books, Vol. 43 No. 21. https://www.lrb.co.uk/the-paper/v43/n21/edan-ring/on-pegasus. Accessed 30.12.2021

Rohde M; Brödner P; Stevens, G; Betz, M; Wulf, V (2017) Grounded Design – a Praxeological IS Research Perspective. Journal of Information Technology (JIT), Vol.32, pp 163-179

Rohde, Markus. (2004). Find what binds: Building Social Capital in an Iranian NGO community system. In Huysman, Marleen and Wulf, Volker: *Social Capital and Information Technology*. MIT Press, pp. 75-111.

Rohde, Markus. (2007). *Integrated Organization and Technology Development (OTD) and the Impact of Socio-Cultural Concepts - A CSCW Perspective.* Ph.D Dissertation. Datalogiske skrifter. University of Roskilde, Denmark, 97ff.

Rohde, Markus. (2013). Trust in Electronically-Supported Networks of Political Activists. Workshop paper in *Proceedings of the 2013 conference on Computer supported cooperative work* (CSCW '13). ACM, New York, NY, USA.

Rohde, Markus; Aal, Konstantin; Misaki, K.; Randall, David; Weibert, A.; and Wulf, V. (2016). Out of Syria: Mobile media in use at the time of civil war. International Journal of Human-Computer Interaction, 32(7), pp. 515-531.

Ronzhyn, Alexander. (2014). The Use of Facebook and Twitter During the 2013–2014 Protests in Ukraine. In *Proceedings of the European Conference on Social Media,* 442-448.

Rosenberg, Matthew; Confessore, Nicholas; and Cadwalla, Carole. (2018). New York Times. "How Trump Consultants Exploited the Facebook Data of Millions". https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Accessed 20 March 2018.

Rosenberg, Tina. (2011). Revolution U: What Egypt learned from the students who overthrew Milosevic. *Foreign Policy*. Retrieved June 05, 2014 from http://foreign policy.com/articles/2011/02/16/revolution_u

Ruiz, J., Serral, E., & Snoeck, M. (2021). Unifying functional User Interface design principles. International Journal of Human–Computer Interaction, 37(1), pp. 47-67.

Rujevic, N. (2017). Serbian government trolls in the battle for the internet. Deutsche Welle. http:// dw.com/en/serbian-government-trolls-in-the-battlefor-the-internet/a-37026533. Accessed 7 June 2019.

Ruoti, S.; Monson, T.; Wu, J.; Zappala, D.; and Seamons, K. (2017). Weighing context and trade-offs: How suburban adults selected their online security posture. In: 13th Symposium on usable Privacy and Security ({SOUPS} 2017). USENIX Association, pp. 211-228

Ruoti, Scott; Andersen, Jeff; Heidbrink, Scott; O'Neill, Mark; Vaziripour, Elham; Wu, Justin; Zappala, Daniel; and Seamons, Kent (2016). We're on the same page: A usability study of secure email using pairs of novice users. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. ACM. pp. 4298-4308.

Saad T; Khan F (2016) Nudging Pakistani users towards privacy on social networks. In: SAI Computing Conference (SAI), 2016. IEEE, pp 1147-1154

Saeed, Saqib; Rohde, Markus; and Wulf, Volker. (2011). Analyzing political activists' organization practices: Findings from a long term case study of the ESF. *International Journal of Computer Supported Cooperative Work (CSCW) 4-5*, 265-304. http://dx.doi.org/10.1007/s10606-011-9144-0

Salaheldeen, Hany and Nelson, Michael. (2012). Losing my revolution: how many resources shared on social media have been lost?. In *Theory and Practice of Digital Libraries*. Springer Berlin Heidelberg, DE, 125-137. http://dx.doi.org/10.1007/978-3-642-33290-6_14

Salaheldeen, Hany and Nelson, Michael. (2013). Resurrecting My Revolution. In *Research and Advanced Technology for Digital Libraries*. Springer Berlin Heidelberg, DE, 333-345. http://dx.doi.org/10.1007/978-3-642-40501-3_34

Sambasivan, Nithya; Checkley, G.; Batool, A.; Gaytán-Lugo, L.S.; Matthews, T.; Consolvo, S.; and Churchill, E. (2018). August. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018). USENIX} Association, pp. 127-142

Sandoval-Almazan, Rodrigo; and Ramon, Gil-Garcia J. (2014). Towards cyberactivism 2.0? Understanding the use of social media and other information technologies for political activism and social movements. In *Government Information Quarterly,* vol. 31, no. 3, pp. 365-378.

Sarajevo Times. (2019). "Several Hundred People gathered on Protests asking for Truth of murdered Dzenan Memic". https://www.sarajevotimes.com/several-hundred-people-gathered-on-protests-asking-for-truth-of-murdered-dzenan-memic. Accessed 06 July 2019.

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it?. O'Reilly.

Schaar, P. (2010). Privacy by design. Identity in the Information Society, 3(2), 267-274.

Schwaber K; Beedle M (2002) Agile software development with Scrum. Pearson International Edition, USA

Senarath, Awanthika; and Nalin AG Arachchilage. (2018). Why developers cannot embed privacy into software systems? An empirical investigation. In Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018, pp. 211-216.

Shama, Shok; and AlMeraj, Zainab Faisal. (2019). An investigation into consumer experiences using e-commerce in the State of Kuwait. In *CHI2019 Workshop Proceedings - With an Eye to the Future: HCI Research and Practice in the Arab World*. March 2019, pp. 45 – 51. https://doi.org/10.1145/3290607.3299006

Sharples, Mike. (1996). An Introduction to Human-Computer Interaction, in M. Boden (ed.)Artificial Intelligence, Academic Press, pp. 293–323.

Shklovski, Irina; and Wulf, Volker. (2018). The Use of Private Mobile Phones at War: Accounts From the Donbas Conflict. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, pp. 386.

Silverstein, Richard. (2018). Israel is shutting down its critics on social media. It happened to me. Middle East Eye. https://www.middleeasteye.net/opinion/israel-shutting-down-its-critics-social-media-it-happened-me. Accessed 10 July 2019.

Singh L; Yang G H; Sherr M; Hian-Cheong A; Tian K; Zhu J; Zhang S (2015) Public information exposure detection: Helping users understand their web footprints. In: Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ACM, pp 153-161

Skinner, Julia. 2011. Social Media and Revolution: The Arab Spring and the Occupy Movement as Seen through Three Information Studies Paradigms. *All Sprouts Content*. Paper 483.

Sloan, J. (1996). The Dayton peace agreement: Human rights guarantees and their implementation. Eur. J. Int'l L., 7, 207.

Smajlović, Ermina; Kamarić, Alma; and Sinanagić, Ahmet. (2015). Social media as a tool for the realization of marketing objectives of higher education institutions in Bosnia and Herzegovina. International Journal of Economics, Commerce and Management, vol. 3, no. 3, pp. 2-13.

Spasimo Kastel. Facebook Group (>3500 members). Retrieved January 04, 2015 from https://facebook.com/spasimokastel

Spiekermann, S. (2012). The challenges of privacy by design. Communications of the ACM, 55(7), 38-40.

Srpskainfo. (2018). "Banjalučka policija podnijela izvjestaj protiv Davora Dragičevića". https://srpskainfo.com/ozbiljne-prijetnje-banjalucka-policija-podnijela-izvjestaj-protiv-davora-dragicevica. Accessed 28 October 2018.

Statcounter. (2018). “Social Media Stats Bosnia And Herzegovina”. http://gs.statcounter.com/social-media-stats/all/bosnia-and-herzegovina. Accessed 18 March 2018.

Steinke, Ines. (2000). Gütekriterien qualitativer Forschung. In *Qualitative Forschung*, Uwe Flick, Ernst von Kardorff and Ines Steinke. Reinbek b. Hamburg, Rowohlt, DE, 319-331.

Stern-Hoffman, G. (2013). Government to use citizens as army in social media war. The Jerusalem Post. Retrieved from http://www.jpost.com/Diplomacy-and-Politics/Government-to-use-citizens-as-army-in-social-media-war-322972. Accessed 20 April 2019.

Stevens, Gunnar; and Wiedenhöfer, Torben. (2006). CHIC - a pluggable solution for community help in context. In *Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles* (NordiCHI '06), Anders Mørch, Konrad Morgan, Tone Bratteteig, Gautam Ghosh, and Dag Svanaes (Eds.). ACM, New York, NY, USA, 212-221. http://dx.doi.org/10.1145/1182475.1182498

Stevens, Gunnar; Veith, Michael; and Wulf, Volker. (2005). Bridging among Ethnic Communities by Cross-cultural Communities of Practice. *Communities and Technologies*. 377-396. http://dx.doi.org/10.1007/1-4020-3591-8_20

Stewart, Leo Graiden; Arif, A. Ahmer; Nied, Conrad; Spiro, Emma S.; and Starbird, Kate. (2017). Drawing the Lines of Contention: Networked Frame Contests Within# BlackLivesMatter Discourse. In: Proceedings of the ACM on Human-Computer Interaction, vol. 1, no. CSCW, pp. 96-1.

Stobert, Elisabeth; and Biddle, Robert. (2014). The password life cycle: User behavior in managing passwords. In 10th Symposium on Usable Privacy and Security (SOUPS 2014), pp. 243-255.

Stutzman F; Gross R; Acquisti A (2014) Silent Listeners: The Evolution of Privacy and Disclosure on Facebook. In: Journal of Privacy and Confidentiality 4, Number 2, pp 7–41

Suárez-Serrato, Pablo; Roberts, Margaret E.; Davis, Clayton; and Menczer, Filippo. (2016). On the Influence of Social Bots in Online Protests, Preliminary Findings of a Mexican Case Study, In International Conference on Social Informatics, pp. 269-278.

Such, Jose M.; and Rovatsos, Michael. (2016). Privacy Policy Negotiation in Social Media. In *ACM Transactions on Autonomous Adapted System*, vol. 11, no. 1, article 4, pp. 29. DOI=http://dx.doi.org/10.1145/2821512

Surk, Barbara. (2019). “In Bosnia, a Father’s Grief Swells Into an Antigovernment Movement“. New York Times. https://www.nytimes.com/2019/01/08/world/europe/bosnia-davor-dragicevic-milorad-dodik.html. Accessed 02 February 2019.

Sutton, Jeannette N.; Palen, Leysia; and Shklovski, Irina. (2008). Backchannels on the front lines: Emergency uses of social media in the 2007 Southern California Wildfires. University of Colorado, pp. 624-632.

Tacchi, Jo, Slater, Don, & Hearn, Gregory (2003) Ethnographic Action Research. United Nations Educational, Scientific & Cultural Organisation.

Tacchi, Jo; Foth, Markus; and Hearn, Greg. (2009). Action research practices and media for development. International Journal of Education and Development Using Information and Communication Technology, vol. 5, no. 2, pp. 32-48. https://eprints.qut.edu.au/14077

Tacchi, Jo; Foth, Markus; and Hearn, Greg. (2009). Action research practices and media for development. *International Journal of Education and Development Using Information and Communication Technology* 5, 2: 32-48.

Tactical Technology Collective, https://tacticaltech.org, last accessed 2018/01/28

TacticalTech. (2019). “Security In-a-Box”. https://tacticaltech.org/themes/digital-security/security-in-a-box. Accessed 02 February 2019.

Tactical Tech, Data Detox, https://datadetoxkit.org/de/home. Accessed 17 August 2021.

Tadic, Borislav; Rohde, Markus; Wulf, Volker; and Randall, David. (2016). ICT Use by Prominent Activists in Republika Srpska. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* - CHI '16. pp. 3364-3377. doi:10.1145/2858036.2858153

Tadic, Borislav; Rohde, Markus; and Wulf, Volker. (2018). Cyberactivist: Tool for Raising Awareness on Privacy and Security of Social Media Use for Activists. In: *International Conference on Social Computing and Social Media*. Springer, Cham. pp. 498-510. doi: 10.1007/978-3-319-91521-0_36

Tadic, Borislav; Rohde, Markus; Wulf, Volker; and Randall, David. (in publication). Security and Privacy Aspects of ICT and Social Media Use by Activists in (Post-) Conflictual Societies. In Special Edition of Computer Supported Cooperative Work (CSCW): The Journal of Collaborative Computing, Springer.

Talhouk, R.; Balaam, M.; Toombs, A. L.; Garbett, A.; Akik, C.; Ghattas, H.; and Montague, K. (2019). Involving Syrian Refugees in Design Research: Lessons Learnt from the Field. In *Proceedings of the 2019 on Designing Interactive Systems Conference*, ACM, pp. 1583-1594.

Tarrow, Sidney G. (2011). Power in movement: Social movements and contentious politics. Cambridge University Press, pp. 6.

Tavory, Iddo; and Timmermans, Stefan. (2014). Abductive Analysis: Theorizing Qualitative Research. University of Chicago Press and http://stefan-timmermans-uj7t.squarespace.com. Accessed 01 March 2019.

Tawil-Souri, Helga. (2012). Digital occupation: Gaza's high-tech enclosure. In *Journal of Palestine Studies,* vol. 41, no. 2, pp. 27-43.

Thaler, Richard H.; Cass R. Sunstein; and John P. Balz. (2013). "Choice architecture." In The behavioral foundations of public policy. Princeton University Press, pp. 428-439.

Thedefenceworks. (2022). https://thedefenceworks.com. Accessed 15.1.2022

Totem. (2021). https://totem-project.org. Accessed 30.12.2021

Transparency International. Facebook Group (>3200 members). Retrieved January 04, 2015 from https://facebook.com/TIBiH

Trepte S; Masur P.K (2016) Cultural differences in media use, privacy, and self-disclosure: research report on a multicultural survey study, University of Hohenheim, Germany

Trombetta, Lorenzo. (2012). Altering Courses in Unknown Waters: Interaction between Taditional and New Media during the First Months of the Syrian Uprising. In: *Global Media Journal. German Edition*, vol. 2, no. 1, pp. 1-13.

Trottier, Daniel. (2012). Social Media As Surveillance: Rethinking Visibility in a. Converging World. Surrey, England: Ashgate Publishing, pp. 213.

Tsaliki L (2016) Tweeting the Good Causes: Social Networking and Celebrity Activism. In: Marshall P.D, Redmond S: A Companion to Celebrity, pp 235-257

Tsay-Vogel, Mina; Shanahan, James; and Signorielli, Nancy. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. New media & society, vol. 20, no. 1, pp. 141-161.

Tufekci, Zeynep; and Christopher Wilson. (2012). Social media and the decision to participate in political protest: Observations from Tahrir Square. In *Journal of communication*, vol. 62, no. 2, pp. 363-379.

Turcilo, Lejla. 2010. Will the Internet set us free: New media and old politics in Bosnia-Herzegovina. *Medianali* 4, 8: 11-22.

Uldam, Julie. (2017). Social media visibility: challenges to activism, Media, Culture & Society, SAGE

ULEX. (2021). https://ulexproject.org/courses_events/the-ecology-of-social-movements-2-2. Accessed 30.12.2021

Universal Declaration of Human Rights. https://www.un.org/en/universal-declaration-human-rights. Accessed 29 September 2018.

USAID Privacy Office, Privacy Impact Assessment, https://www.usaid.gov/sites/default/files/SocialMediaPIA.pdf, last accessed 2017/06/17

Ustav Bosne i Hercegovine. 1995. Retrieved December 28, 2015 from http://oscebih.org/dejtonski_mirovni_ sporazum/SR/annex4.htm

Vaskovic, Slobodan. (2018). “Smrtonosne prijetnje Davoru i učesnicima okupljanja, podvučene nacističkim pozdravom”. http://slobodanvaskovic.blogspot.com/2018/07/smrtonosne-prijetnje-podvucene.html. Accessed 28 October 2018.

Vaziripour Elham; Wu, J.; Farahbakhsh, R.; Seamons, K.; O’Neill, M.; and Zappala, D. (2018). Private But Not Secure: A Survey Of the Privacy Preferences and Practices of Iranian Users of Telegram. USEC 2018

Vecernji List. (2017). Vise portala i facebook profila iz Hercegovine blokirano. https://www.vecernji.hr/vijesti/vise-portala-i-facebook-profila-iz-hercegovine-blokirano-1211916. Accessed 18 March 2018.

Vedrana Kulaga. Glas Srpske. (2019). Skajp i vajber uskoro pod pratnjom policije, https://www.banjaluka.com/aktuelno/bih/skajp-i-vajber-uskoro-pod-pratnjom-policije. Accessed 18 July 2019.

Vlachokyriakos, Vasillis; Crivellaro, C.; Wright, P.; Karamagioli, E.; Staiou, E. R.; Gouscos, D.; and Lawson, S. (2017). CHI, Solidarity Movements and the Solidarity Economy. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. ACM, pp. 3126-3137.

Voida, Amy. (2011). Shapeshifters in the voluntary sector: exploring the human-centered-computing challenges of non-profit organizations. *interactions* 18, 6 (November 2011), 27-31. http://dx.doi.org/10.1145/2029976.2029985

Voida, Amy; Harmon, Ellie; and Al-Ani, Ban. (2011). Homebrew databases: complexities of everyday information management in non-profit organizations. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11). ACM, New York, NY, USA, 915-924. http://dx.doi.org/10.1145/1978942.1979078

Voida, Amy; Harmon, Ellie; and Al-Ani, Ban. (2012). Bridging between organizations and the public: volunteer coordinators' uneasy relationship with social computing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '12). ACM, New York, NY, USA, 1967-1976. http://dx.doi.org/10.1145/2207676.2208341

Vukic, Uros. (2018). Nezavisne Novine. "Nikšić uhapšen zbog prijetnji Dragičeviću i zolje". https://www.nezavisne.com/novosti/hronika/Niksic-uhapsen-zbog-prijetnji-Dragicevicu-i-zolje/503470. Accessed 28 October 2018.

Wang Y; Leon PG; Scott K; Chen X; Acquisti A (2013) Privacy nudges for social media: an exploratory Facebook study. In: Proceedings of the 22nd international conference on World Wide Web companion, ACM, pp 763-770

Wang, Q. E.; Myers, M. D.; and Sundaram, D. (2013). Digital natives and digital immigrants. Business & Information Systems Engineering, 5(6), pp. 409-419.

Wang, Yambo; Min, Qingfei; and Han, Shengen. (2016). Understanding the effects of trust and risk on individual behavior toward social media platforms: A meta-analysis of the empirical evidence. In Computers in Human Behavior, vol. 56, pp. 34-44.

Warwick University. (2017). "Information Security Awareness Questionnaire". http://warwick.ac.uk/services/gov/informationsecurity/questionnaire. Accessed 17 June 2017.

Waters, Richard; and Lo, Kevin. (2012). Exploring the Impact of Culture in the Social Media Sphere: A Content Analysis of Nonprofit Organizations' Use of Facebook. *Journal of Intercultural Communication Research*, 41: 297-319. http://dx.doi.org/10.1080/17475759.2012.728772

Wearesocial. (2021). https://wearesocial.com/jp/blog/2021/10/social-media-users-pass-the-4-5-billion-mark. Accessed 8.1.2022

Wessel, L.; Gersch, M.; and Harloff, E. (2017). Talking past each other. Business & Information Systems Engineering, 59(1), pp. 23-40.

Whitten, Alma; and Doug, Tygar J. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. USENIX Security Symposium, vol. 348.

Wilson, Paul. (1991). Computer Supported Cooperative Work: An Introduction. Springer Science & Business Media. ISBN 9780792314462.

Witte, Kim. (1994). Fear control and danger control: A test of the extended parallel process model (eppm). Communications Monographs, vol. 61, no. 2, pp. 113-134

Witzel, Andreas, and Reiter, Herwig (2012). The problem-centred interview. Sage.

Witzel, Andreas. (2000). Das problemzentrierte Interview. In *Forum:Qualitative Sozialforschung*, 1, 1, Article 22.

Wong, Richmond Y.; and Deirdre K. Mulligan. (2019). Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of CHI. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1-17.

Wright, Rebecca N. (2000). Obstacles to freedom and privacy by design. In Proceedings of the 10th conference on computers, freedom and privacy: challenging the assumptions, pp. 97-100.

Wulf, Volker; Aal, Konstantin; Abu Kteish, Ibrahim; Atam, Meryem; Schubert, Kai; Rohde, Markus; Yerousis, George P.; and Randall, David. (2013). Fighting against the wall: social media use by political activists in a Palestinian village. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13). ACM, New York, NY, USA, pp. 1979-1988. http://dx.doi.org/10.1145/2470654.2466262

Wulf, Volker; Misaki, K.; Aal, Konstantin; and Rohde, Markus. (2014). Mobile Media Use in the Zone of Conflict Findings from Early Phases of the Syrian Civil War, IISI - International Institute for Socio-Informatics, vol. 14, no. 2, ISSN 1861-4280

Wulf, Volker; Misaki, Kaoru; Atam, Meryem; Randall, David; and Rohde, Markus. (2013). 'On the ground' in Sidi Bouzid: investigating social media use during the Tunisian revolution. In *Proceedings of the 2013 conference on Computer supported cooperative work* (CSCW '13). ACM, New York, NY, USA, pp. 1409-1418. http://dx.doi.org/10.1145/2441776.2441935

Wulf, Volker; Müller, Claudia; Pipek, Volkmar; Randall, David; Rohde, Markus; and Stevens, Gunnar. (2015). Practice-based Computing: Empirically-grounded Conceptualizations derived from Design Case Studies. In: Wulf V, Schmidt K, Randall D (eds): Designing Socially Embedded Technologies in the Real-World, Springer, London, pp. 111-150.

Wulf, Volker; Pipek, Volkmar; Randall, David; Rohde, Markus; Schmidt, Kjeld; and Stevens, Gunnar. (2018). Socio-Informatics: A Practice-Based Perspective on the Design and Use of IT Artifacts, ISBN: 9780198733249

Wulf, Volker; Rohde, Markus; Pipek, Volkmar; and Stevens, Gunnar. (2011). Engaging with practices: design case studies as a research framework in CSCW. In *Proceedings of the ACM 2011 conference on Computer supported cooperative work* (CSCW '11). ACM, New York, NY, USA, 505-512. http://dx.doi.org/10.1145/1958824.1958902

Xu, Ying; and Maitland, Carleen. (2019). Participatory data collection and management in low-resource contexts: a field trial with urban refugees. In Proceedings of the Tenth International Conference on Information and Communication Technologies and Development (ICTD '19), ACM, New York, NY, USA, pp. 18. DOI: https://doi.org/10.1145/3287098.3287104

Yang, Guobin. (2018). (Un) civil Society in Digital China| Demobilizing the Emotions of Online Activism in China: A Civilizing Process. International Journal of Communication, 12, pp. 21.

Yeratziotis, A.; Pottas, D.; and Van Greunen, D. (2012). A usable security heuristic evaluation for the online health social networking paradigm. International Journal of Human-Computer Interaction, 28(10), pp. 678-694.

Yi, Mun Y.; and Fred D. Davis. (2003). Developing and validating an observational learning model of computer software training and skill acquisition. In *Information Systems Research*, vol. 14, no. 2, pp. 146-169.

Yongick, Jeonga; and Yeuseung, Kim. (2017). Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. Computers in Human Behavior, vol. 69, pp. 302-310.

Yoo, Daisy; Lake, Milli; Nilsen, Trond; Utter, Molly E.; Alsdorf, Robert; Bizimana, Theoneste; Nathan, Lisa P.; Ring, Mark; Utter, Elizabeth J.; Utter, Robert F.; and Friedman, Batya. 2013. Envisioning across generations: a multi-lifespan information system for international justice in Rwanda. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13). ACM, New York, NY, USA, 2527-2536. http://dx.doi.org/10.1145/2470654.2481349

Zeng, Eric; Shrirang Mare; and Franziska Roesner. (2017). End user security and privacy concerns with smart homes. In 13th Symposium on Usable Privacy and Security ({SOUPS} 2017), pp. 65-80.

Zhou, Z.; Bandari, R.; Kong, J.; Qian, H.; and Roychowdhury, V. (2010). Information resonance on Twitter: watching Iran. In *Proceedings of the First Workshop on Social Media Analytics*. ACM. pp. 123-131.

Ziegele, Marc; and Quiring, Oliver. (2011). Privacy in social network sites. In: *Privacy Online: Perspectives on privacy and self-disclosure in the Social Web*, Springer, pp. 5-189.

Zimmer, Eric. A. (2003). Understanding a Secondary Digital Divide: Nonprofit Organizations and Internet Bandwidth Connectivity. In Trends in Communication 11, 1: 81-94, http://dx.doi.org/10.1207/S15427439TC1101_06

Zuboff, Shoshana. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books.