IEEE SSIT SOCIETY ON SOCIAL IMPLICATIONS OF TECHNOLOGY

2018 IEEE International Symposium on Technology in Society (ISTAS) Proceedings
Miriam Cunningham and Paul Cunningham (Eds)
ISBN: 978-1-5386-9479-4

Cybersecurity for Civil Society

Pavan K. Jagalur, Peter L. Levin, Kate Brittain, Matthew Dubinsky, Kristine Landau-Jagalur, Charlotte Lathrop
Amida Technology Solutions, Inc.
Washington, DC
Email: pavan@amida.com, peter@amida.com

***Abstract* - This paper explores emerging security and privacy challenges faced by Civil Society Organizations (CSOs), particularly those advocating for democracy or human rights within closing spaces, such as conflict zones or surveillance states. We met with CSOs and experts in democracy and governance to understand their challenges and concerns. Informed by experience developing information security best practices, we propose alternative design patterns based on their input that will help the technology industries, security professionals, and advocacy groups better address CSOs' most pressing security and privacy needs.**

Our contention is that security guidance offered by professionals from democratic societies is ineffective for closing spaces due to ignorance of their environments and assumptions that do not apply outside a liberal-democratic context. For resource-constrained CSOs with limited capacity for strategic planning, traditional approaches have proven difficult to apply. We introduce an alternative approach focused on expanding security literacy and improving software design patterns.

Keywords - Arab Spring, Censorship, Civil Society, Closing Spaces, Color Revolution, Corruption, Cybersecurity, Digital Governance, Fake News, Free Speech, Great Firewall, Information Technology, Information Technology, Non-Governmental Organizations, Open Internet, Open Government, State Propaganda, Social Media Activism

I. INTRODUCTION

Civil society, or the "third sector" (after government and private business), comprises a wide range of affiliate groups and associations. These include informal social groups (like spiritual groups or sports clubs), large advocacy groups and non-governmental organizations (NGOs) (like Amnesty International or faith-based organizations), and loosely organized professional communities such as the press or academia. In general, civil society functions as a public sphere, in which society collectively discusses, advocates for, and fulfills needs and values that may be underprovided by the public and private sectors [1]. Civil Society Organizations, a subset of NGOs, serve a critical role by ensuring that their communities can peacefully organize to have their needs and concerns addressed.

Information technology (IT) has radically altered how people learn, communicate, and share ideas. New information communications technologies (ICTs)[1] have altered the balance of power between formal levers of authority and the popular will, as expressed through civil society. They have played a well-publicized role in rousing social upheavals around the world, from the Color Revolutions and the Arab Spring to the use of micro-targeted[2] misinformation campaigns to sway elections.

Many ICT platforms were developed as tools for communication, entertainment, or productivity. Their information-sharing capabilities, however, enabled fringe movements to amplify their voices, radicalize vulnerable communities, and coordinate or promote violent or extremist activities. Regulatory bodies and social conventions have been slow to grapple with the security and privacy implications of ICTs, as well as their broader societal impacts.

While governments in open societies endeavor to manage these changes in accountable and transparent ways, countries with adversarial attitudes toward freedom of assembly and speech exert control through censorship, blacklists of citizens, and electronic surveillance of activities and private communications. States adopting such approaches are termed "closed" or "closing" spaces due to their opacity and lack of openness to public input. These efforts can compromise the security and privacy of their people, erode civic autonomy, and promote opacity in government that fosters corruption, abuse, and violence. The same technologies used by organizations to protect their networks from intrusion or misuse can, when applied by a governmental authority intent on suppressing opposition, be used to limit expression and civic engagement.

CSOs play an indispensable role in maintaining transparency, enabling community organization, and publicizing incidences of malfeasance. Amida has engaged in informal discussions with CSO staff as well as experts in geopolitics and cybersecurity to determine the particular security challenges, threat environments, and concerns faced by organizations in closing spaces[3]. We have come to

[1] ICTs include platforms like social media, content delivery tools, and direct messaging tools.
[2] A marketing strategy that uses consumer data and demographics to identify the interests of specific individuals or very small groups of like-minded individuals in order to influence their thoughts or actions.
[3] While governments in more open societies have also expanded scope for regulation and data collection, CSOs in closing spaces face specific strategies

understand that traditional security paradigms, with a disproportionate focus on operational and fiduciary risks to public or private organizations, often ignore the broader risks that accrue to the public or to society. As a result, much of the guidance and effort from the information security field is inadequate to the needs of CSOs due to the nature of the work they do and the unique threat environments they face.

We propose that international communities, information security professionals, and technology industries must partner with CSOs to confront these threats. They must also develop better mechanisms for raising "security literacy" by pioneering design patterns that convert secure processes into intuitive workflows, rather than simply adding layers of tools or oversight.

This paper will present a general description how CSOs operate followed by an overview of traditional security patterns and the ways in which they fail to account for CSO's operational contexts. It will then provide a broad overview of the most prominent techniques and strategies used by governments in closing spaces that threaten CSOs followed by a description of specific challenges CSOs face in facing these threats. The paper concludes with a description of an alternative, non-traditional approach to organizational security and the roles different actors may play to implement them.

II. The Civil Society and CSO Environment

CSOs operate differently from peers in the public and private sectors due to differences in their missions, underlying values, and how they access resources. CSOs often serve marginalized groups, like religious minorities and indigenous populations. Because they are not-for-profit, they rely on a combination of private donations and public support. Local donations and, if available, state funding may be insufficient to maintain and operate the organizations, so many CSOs solicit resources from international interest groups, foreign governments, and multilateral institutions, like the European Union and the United Nations. Shifting international tensions and suspicion of foreign influence can hamper their ability to operate safely, and governments in closing societies may limit or prevent outside funding and assistance from reaching domestic CSOs.

Large international organizations often partner with smaller, local CSOs to benefit from specialization, provide direct services, or leverage local contacts and expertise. When large organizations are forced to withdraw from regions, it can severely diminish the capacities of local partners, regardless of whether they directly receive support. The interdependencies among these organizations can mean that reduction in capacity for one entity can weaken many others, limiting the development, organizational maturity, and sophistication of an entire regional network.

CSOs leverage the near-ubiquitous access and user-friendly nature of ICTs, such as social media platforms, to disseminate information, raise awareness, and organize around critical issues that may be restricted by formal channels. Since CSOs often work on controversial issues and stand at an intersection of the government, the public, and private sectors, they are particularly susceptible targets for repression and manipulation. The same technologies that expand access and open channels for communication can be weaponized by governments to directly suppress dissent, censor or cover up information, and diminish the scale, maturity, and influence of CSOs' efforts.

III. Traditional Security Patterns and Their Deficiencies

The information security field has evolved to better serve a variety of different organizations, environments, and missions, yet it remains slanted toward the perspectives of the organizational cultures where it was initially systematized. Security processes were first codified within the defense and intelligence communities before expanding into law enforcement, finance, civilian agencies, and the private sector. Its paradigms are rooted in systemic biases and assumptions that are incongruent to the culture of CSOs, impractical within closing spaces, or ineffective under state surveillance.

These biases suffuse, often in subtle ways, much of the conventional thinking around security. This impacts how experts develop threat models and prioritize risks, and the mechanisms they use to address weaknesses once uncovered. Traditional frameworks conceptualize organizational data as an "information asset" that emphasizes monetary, reputational, or strategic value to the organization. These assets are positioned along various "attack surfaces," or the sum of all points through which an attacker can gain access (e.g. physical hardware, network infrastructure). They assume the primary threats to these assets are "adversaries" and "insider threats" seeking to compromise the confidentiality, integrity, or availability of this information for pecuniary, geostrategic, activist, or mischievous ends.

These assumptions have led to traditional frameworks and activities focused on "policing," in which the organization goes about its business while security operates as a separate entity, vigilant for adversaries. This vigilance focuses on the organization's network and IT systems with the implicit understanding that protecting these attack surfaces naturally protects the data within. Information security is enacted through specific policies and enforced by oversight mechanisms such as system authorization, log review, or vulnerability scanning, often with little consideration for enabling the mission. Oversight is usually accomplished through the application of additional technologies for auditing and assurance. This mechanistic, top-down model casts security incidents as the preventable consequences of operational failures, policy violations, exploited vulnerabilities, and "human error," a catch-all term for any mistakes or lapses in judgement.

Such assumptions do not neatly apply to CSOs, especially in closed societies. They are often motivated by passion for their cause and may not be accustomed to valuing their resources in quantifiable terms. Likewise, threat models that prioritize risks by organizational impact are of limited utility when many risks are existential, resulting in dissolution of the

---

of state suppression that merit special attention and concern. The effects of expanding data collection more broadly should be addressed as a subject for a broader analysis.

organization, social ostracism, or imprisonment of or violence against the organization's stakeholders.

Moreover, their relationships with their governments are rarely entirely adversarial. Intrusions may seek to exert control over the organization's activities rather than disrupting them. Traditional approaches, preoccupied with narrowly defined risks to the organization from adversaries, ignore risks from "malicious allies," as well as secondary effects to society such as the spread of misinformation, chilling effects[4] on speech, or *de facto* constraints on issue advocacy.

The prioritization of IT and administration as primary security mechanisms breaks down as well. CSOs often work in partnership with local, regional, and international contacts. They routinely exchange large volumes of information with other organizations, lawyers, journalists, organizers, activists, or translators. Each of these entities have their own security approaches and threat environments that the organization cannot account for but must communicate with nevertheless. Effective security under these circumstances must account for the physical security of materials and all the ways information moves across organizational boundaries and attack surfaces.

IV. State Based Strategies for Closing Civic Spaces

The level of surveillance and the nature of suppression to which CSOs are subjected varies based on factors such as level of development and infrastructure, the political aims of the ruling government, and the state's capacity and control over its territory.

A. Control Over Network Infrastructure

The People's Republic of China (PRC) maintains the most sophisticated technological infrastructure for state-directed influence over the digital commons. Its techniques, technologies, and values regarding the internet's role in public life are replicated throughout the world by nations that share the Communist Party of China's (CPC) governance approach. Its strategies serve as a benchmark for the guiding philosophies and practical methodologies of governments in more-closed spaces. While these techniques are not limited to the PRC, it is where the most well-developed and comprehensive implementations of them can be found.

In contrast to Western norms, which conceptualize the Internet as a "global village" that operates irrespective of territorial borders or physical boundaries, the CPC views the West's *de facto* dominance over popular Internet platforms and user-facing software as an impingement on its national sovereignty [2]. Consequently, cyber capabilities are critical planks of Chinese national security policy and are strategically implemented through a series of public works programs collectively known as the "Golden Shield Project." These programs employ a suite of censorship and offensive cyber capabilities as well as mechanisms for society-wide cultural engineering.

[4] The inhibition or discouragement of the legitimate exercise of natural and legal rights by the threat of legal or informal sanction.

The CPC's censorship capabilities rely on a nation-wide network architecture of servers and routers through which all internet traffic is routed [3]. Traffic passing through this gateway, colloquially known as the "Great Firewall," is subject to three main defensive forms of control or manipulation:

1. Blockage of Internet Protocol (IP) addresses, ports, and protocols to prevent general site access.
2. Domain Name Service (DNS) poisoning and injection to redirect users to pages other than what was originally requested, to block access by locking the request in a redirect loop, or to stage an alternative, censored version of the page.
3. Deep packet inspection of internet traffic to block blacklisted IPs or keywords. Tools for circumvention of the "Great Firewall," such as VPN, encrypted email, or proxy services, must be pre-approved by the government or they will also be blocked [4].

The "Great Cannon," China's primary offensive capability, can be used to inject malicious traffic or to suppress traffic using man-in-the-middle techniques [5]. It can be used for eavesdropping, transmitting artificial requests, or executing denial-of-service attacks.

B. Suppression of Dissenting Speech

Nominally democratic governments can suppress civic dissent using combinations of cyberattacks, spying, and physical intimidation. Activists in the United Kingdom [6], Canada [7], and United States [8] have reported monitoring and surveillance by law enforcement through phone tapping and chat and email transcription. Commercial spyware companies offer turnkey solutions marketed toward nation-states to reduce crime, prevent terrorism, and maintain public safety by gaining access to information from remote PCs. These tools are used to compromise the social media accounts and hardware of journalists or activists and their known associates. As demonstrated by the Ethiopian government's crackdown on the Oromia Media Network (OMN) in 2016 [9], governments can constrain the spread of information and silence marginalized populations through a strategic combination of jamming news networks, deploying sophisticated malware attacks, and harassing critical voices throughout the diaspora.

C. Regulatory Suppression and Social Control

State actors are better resourced, and more patient, than commercial or non-governmental adversaries, and their intrusion is backed by lawful authority. These advantages can manifest as onerous legal requirements that divert resources from productive work or as direct intimidation and investigation by police. For example, many governments impose laws and regulations that make organizations liable for their own content. Private organizations can be subjected to harsh penalties for the content they host or for even interacting with unaffiliated participants that violate censorship rules [10]. In some cases, these penalties can be imposed through social sanction. A formalized version of this is being piloted in China through an experimental "Social Credit" system based on data collected from social networks, online shopping, and

eventually facial recognition [11]. These data can be used to evaluate citizens based on behavior, personal associations, and consumptive preferences. Resulting scores are tied to benefits, such as access to credit or employment, and can be used to suppress expression from marginalized groups by penalizing disapproved perspectives.

D. Conflict Zones

Organizations working on documenting human rights abuses, as in conflict zones, must not only secure their personnel, they must also secure collected data, the conveyance of those data, and the (typically extraterritorial) servers on which the data is stored. Furthermore, governments can destroy or disable telecommunications infrastructure in conflict zones, necessitating improvised solutions and workflows. For example, the Syrian government shuts down access to the internet and cellular connections for regions in advance of an attack, limiting residents' ability to communicate or coordinate with each other for help [12]. Compromise at any phase endangers the lives of those involved, as well as their families and associates. Many of the security paradigms for non-military organizations are based upon the potential for monetary loss and rarely consider the real, physical consequences these people face.

V. CSO Capacity Contraints

CSOs are constrained in their ability to engage in long-term security strategy and contingency planning due to their constantly shifting operating environments. In addition, CSOs face immense pressure from funders and the public to apply as much of their budgets as possible directly toward their stated missions, while minimizing overhead costs or "operational" investments. While some may save staff time by outsourcing security to IT professionals, many CSOs report difficulty in finding support that is both skilled and trustworthy enough to handle sensitive information [13]. If investment in information security is perceived as optional overhead, rather than as an essential element of mission-driven work, staff will opt to focus on more immediate or rewarding priorities.

Even large, well-funded organizations — including US government agencies — have poor records with day-to-day security. Approximately eighty-percent of successful cyber incidents at the U.S. Department of Defense were traceable to poor user practices, poor network management, or vulnerable network architecture [14]. When mature, security-focused organizations are unable to execute on the fundamentals, it should not be surprising that CSOs find it all but impossible. The standard responses to mitigate gaps along the "human attack surface" include security audits, authorization processes, training and awareness campaigns, background checks, and intensive monitoring of network activity. Many of these approaches are not only limited, but prohibitively expensive or impractical for small- or medium-sized CSOs.

Capacity constraints manifest in other, subtle, ways as well. While organizations traditionally use "capacity" to refer specifically to technical resources, budget, or available staff, CSOs exist within a broader social context and inherit safeguards from the societies around them, such as protections against arbitrary search and seizure, mores regarding privacy or attorney-client privilege, and reliable access to critical network infrastructure. On a practical level, this means an organization's own staff must shoulder the responsibility of protecting not only the information assets, but themselves and their families with fewer resources than other ICT-dependent enterprises.

Security experts and hackers continue to develop new strategies to address the gaps in practice and technology. But, they often neglect the challenges faced by organizations that do not fit the stereotypical model of an institutional customer of security services. Even CSOs that manage to sort through conflicting advice and stay up-to-date with security best practices often find them difficult to implement due to technology debt, lack of organizational capacity, and technical complexity [15]. In addition, CSOs with limited capacity are frequently unable to develop and implement policies, as the urgency of their circumstances and the uncertainty of their funding streams precludes the kinds of thoughtful process engineering or long-term planning needed to sustainably operationalize security.

VI. Securing the Human Attack Surface

As CSOs have limited financial resources, insisting that they "use more technology" to fix their existing technology is both infeasible and tin-eared. Moreover, reactive approaches to security incursions are of limited utility as incidents can be existential threats to the organization, dangerous for its staff, or leave blind spots that their administrative processes cannot detect. In the absence of sophisticated technical oversight (or policy enforcement), CSOs must explicitly train their staff to better understand the privacy and security implications of their actions. This is not to say that technical and engineering solutions, like prioritizing end-to-end encrypted communication channels, are not crucial. Rather, focusing on awareness and education will make it easier to integrate best practices, like multi-factor authentication, into organizations' workflows.

Security and privacy are not isolated considerations. CSOs should train their staff, their partner organizations, and their stakeholders to become more fluent in basic risk management. Security professionals should assist them by providing the training and process engineering required to develop better habits.

Diffusing these practices will require innovations that we believe can be achieved with attention, investment, and focus. Software developers and technical experts must better understand how CSOs in conflict zones and closing societies differ from their stereotypical clients. They must prioritize security and privacy in their product development and pioneer design patterns and functionality that better account for these contexts. Usability and accessibility are crucial for mainstream adoption, and security-related features should be simple to use. The most thorough email encryption will fail if users cannot differentiate between a public and private security key or find a password manager interface too cumbersome. The most effective security practice is, by definition, the one to which the least trained or most careless member adheres.

VII. Converging Disciplines

A. Security and IT Professionals

Organizations, such as Frontline Defenders [16] and the Committee to Protect Journalists [17], already provide resources on security tools, tactics, and software for people operating on the ground. For example, the Security in a Box guide, developed through a collaboration by Frontline Defenders and the Tactical Technology Collective, constitutes an excellent framework for providing actionable guidance that is understandable and easy to deploy [18]. The information is presented in a straightforward manner and the number of options presented are limited and avoid overwhelming readers with choices. Most importantly, the guide presents important context for when and how to use these tools to support a non-technical audience. It is limited, however, because it places the onus of maintaining security on already harried front-line workers. Dispensing guidance only in this way leads to haphazard and inconsistent adoption within teams and organizations. Inconsistency promotes chaotic workflows, miscommunication, and security standards that are only clumsily maintained, if at all.

Security guidance should enable the people within CSOs to make more informed decisions about the risks and consequences that result from their actions while minimizing the number of decisions placed in their hands. The majority of security gaps do not require specialized technical expertise, only structured, easy-to-implement processes that encourage best practices as a matter of course. Manuals should provide simple and prescriptive guidance for CSO leadership about which tools to use, what policies work best, and how to communicate and operationalize procedures throughout an organization. Operating environments are heterogenous, so guidance must be well tailored and localized for their (non-technical) audience. This can be done by providing nested decision-trees[5] to help leaders find the tools that are right for their organizations' scale and workflows, and by providing important context to help them understand the trade-offs of different options.

B. Technology Providers

To broaden security awareness in closed societies, the technology sector must foster adoption of mainstream security and privacy-enhancing features. These features, such as end-to-end encryption[6], granular privacy controls, or a "right to be forgotten" are often dismissed as appealing only to a niche market. As a result, they are typically served by specialized tools geared toward technical users and, consequently, lag far behind their mainstream peers in usability, interoperability, and reliability. The principles of "universal design"[7] teach us that design innovations intended to support vulnerable groups can often benefit society as a whole. In the same way that sidewalk ramps, originally developed for wheelchair accessibility, can also enable parents to more easily push strollers, software that provides secure interaction patterns for closed environments can benefit the user-base in more open societies as well [19]. [8]

Services that facilitate information sharing and data collection should develop strong privacy policies communicated in simple, localized, language. These policies should not only enumerate expectations between the provider and the user, but also the privacy impact of the data, and whether third parties (state authorities, business partners, or members of their communities and professional networks) can view and analyze it. In addition to stronger privacy policies, services should strive to provide more granular privacy controls and develop interaction patterns that encourage good security habits and cultivate sensitivity around data privacy. For example, uploading photos to social media can transmit a great deal of metadata attached to the photo, including location, time and date stamps, and a device fingerprint. Rather than obfuscating the amount of sensitive information being transmitted, design patterns for uploading documents should make it clear whether geolocation data or other potentially compromising information is being transmitted. Here, specifically, platforms should provide options to screen or anonymize such information wherever possible.

C. Democracy & Governance Organizations

In addition to providing guidance to CSOs, security professionals consult with democracy and governance organizations to craft public information campaigns. These large international organizations are often only capable of providing technical assistance to the largest and best-resourced CSOs in their target countries, leaving smaller organizations and marginalized groups without support. The technical assistance provided often manifests in the form of in-country and offshore training programs. These can provide ideal venues for creating and distributing information about secure practices and tools, as well as capacity building strategies. They also offer opportunities for CSO staff to network and learn from similar organizations in other countries. When training programs provide shareable, localized, and easily duplicable materials, attendees can distribute information to colleagues in their home countries to improve awareness.

While training programs are an important way for the international community to support CSOs, the funding streams and evaluation metrics that donors use often do not align with these goals. As overhead is used as a crude metric for how efficiently CSOs spend donor money, investments in long-term capacity building, training programs, or technology solutions with large front-end costs are disincentivized. Security and privacy are irreplaceable overhead costs. Grants or metrics for monitoring and evaluation should be structured to incentivize, not penalize, organizations with cybersecurity foresight.

[5] Decision support tool displaying decisions and potential consequences through a tree-like graph or model.

[6] Note: While encryption is critical for privacy and anonymity, it cannot indefinitely guard against anyone with sufficient computing power at their disposal. Discretion should be maintained with extremely sensitive information.

[7] The term was coined by the architect Ronald Mace to describe the concept of designing all products and the built environment to be aesthetic and usable to the greatest extent possible by everyone, regardless of age, ability, or status in life.

[8] A design principle referred to as "the curb cut effect."

VIII. Conclusion

The security and privacy challenges for CSOs in closed societies are compounded by their relationship to their adversaries and the nature of their threat environments. Unlike many organizations with comparable levels of risk exposure, CSOs have far less capacity to address security risks and challenges. Worse yet, many are small, meagerly funded, and lack staff with the technical expertise to keep abreast of shifting developments in technology. As security and technical tasks are not core competencies, their ideas about how to manage risks can often be hampered by lack of knowledge, outdated information, or crude heuristics that are ineffectual against state surveillance strategies. Even with up-to-date information and technically proficient staff, they often lack the organizational capacity to understand what new developments mean for them or to develop strategic plans and processes to remediate them.

Addressing these unique security concerns will require collaboration among security, software development, and international development stakeholders. Donors and international organizations that focus on democracy and governance must better equip themselves to guide and train CSOs managing internal security. In the same vein, the security and technology industries must do a better job of understanding the needs of users in closing spaces and providing tools and capabilities that allow them to better manage information risk. International donors, organizations, and the technology industry can strengthen civic spaces and public engagement around the world by providing technical guidance and encouraging the promotion of information security best practices. CSOs have a critical role to play in the society of each country, and the vibrancy of this community is critical to maintaining accountable governance, free speech, and the protection of human rights. It is imperative that the technology industry and the international community adapt to protect those struggling to maintain this civic space, even as some nation-states attempt to constrain the public sphere.

Acknowledgment

We wish to acknowledge Syla Mummidi, Sergio Orellana, Jacqueline Medina, Servio Medina, and Emilie Riggs for their expertise and support throughout this project. In addition, special thanks to the anonymous CSO representatives and Democracy and Governance experts who took risks to speak with our team about this sensitive topic.

References

[1] Habermas, J. *The Structural Transformation of the Public Sphere*. The MIT Press. 1991.

[2] Shen, F. "Great Firewall of China." In Harvey, K. Encyclopedia of Social Media and Politics. SAGE, Volume 2, 599-602. 2014. Available: https://www.researchgate.net/profile/Fei_Shen6/publication/281030754_Great_Firewall_of_China/links/55d1ba4f08aee5504f68ed36/Great-Firewall-of-China.pdf. [Accessed: June 27, 2018].

[3] Bu, R. "The Great Firewall of China." Murray State University. 2013. Available: http://campus.murraystate.edu/academic/faculty/wlyle/540/2013/Bu.pdf. [Accessed: June 27, 2018].

[4] Winter, P and Lindskog, S. "How the Great Firewall of China is Blocking Tor," In Proc. USENIX Workshop on Free and Open Communications on the Internet. 2012. Available: https://www.usenix.org/conference/foci12/workshop-program/presentation/winter. [Accessed: June 27, 2018].

[5] Marczak, B.; Weaver, N.; Dalek, J.; Ensafi, R.; Fifield, D.; McKune, S.; et al. "An Analysis of China's 'Great Cannon.'" USENIX Workshop on Free and Open Communications on the Internet. 2015. Available: https://www.usenix.org/conference/foci15/workshop-program/presentation/marczak. [Accessed: June 27, 2018].

[6] Bowcott, O. "GCHQ spied on Amnesty International, tribunal tells group in email." The Guardian. 2015. Available: https://www.theguardian.com/uk-news/2015/jul/01/gchq-spied-amnesty-international-tribunal-email. [Accessed: June 29, 2018].

[7] Zwibel, C. and Gill, L. "Why does Canada spy on its own indigenous communities?" 2017. Available: https://www.opendemocracy.net/protest/surveillance-indigenous-groups-canada. [Accessed: June 29. 2018].

[8] Oke, F. "Confidential: Surveilling Black Lives Matter". Aljazeera. 2017. [Accessed: June 27, 2018].

[9] Marczak, B.; Alexander, G.; McKune, S.; Scott-Railton, J.; and Deibert, R. "Champing at the Cyberbit." The Citizen Lab. 2015. Available: https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/. [Accessed: June 27, 2018].

[10] Chew, W. "How It Works: Great Firewall of China." Medium. Available: https://medium.com/@chewweichun/how-it-works-great-firewall-of-china-c0ef16454475. [Accessed: June 27, 2018].

[11] Mistreanu, S. "Life Inside China's Social Credit Labrotory." Foreign Policy. 2018. Available: https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/. [Accessed June 27, 2018].

[12] Freedom on the Net 2017. "Syria *Country Profile*". Freedom House. Available: https://freedomhouse.org/report/freedom-net/2017/syria. [Accessed: June 29, 2018].

[13] Kazansky, B. "Digital Security in Context." Tactical Technolgoy Collective. p. 26. 2015. Available: https://secresearch.tacticaltech.org/media/pages/pdfs/original/DigitalSecurityInContext.pdf. [Accessed: June 27, 2018].

[14] "Department of Defense Cybersecurity Culture and Compliance Initiatve." Office of the Secretary of Defense. 2015.

[15] Kazansky, B. "Digital Security in Context." Tactical Technolgoy Collective. p. 5. 2015. Available: https://secresearch.tacticaltech.org/media/pages/pdfs/original/DigitalSecurityInContext.pdf. [Accessed: June 27, 2018].

[16] "Digital Protection." Front Line Defenders. 2017. Available: https://www.frontlinedefenders.org/en/programme/digital-protection. [Accessed: June 27, 2018].

[17] Smyth, F. *Journalist Security Guide*. 2012 Committee to Protect Journalists. Available: https://cpj.org/security/guide.pdf. [Accessed: June 27, 2018].

[18] "Security In a Box – Digital Security Tools and Tactics." Tactical Technology Collective and Front Line Defends. Available: https://securityinabox.org/en/. [Accessed: June 27, 2018].

[19] Blackwell, A. "The Curb Effect." *Stanford Social Innovation Review*. Available:http://ccf.ny.gov/files/8915/1302/7403/The_Curb_Cut_Effect.pdf. [Accessed: June 27, 2018].