11 Battling the bear

Ukraine's approach to national cyber and information security

Aaron Brantly

Ukraine (Україна, Ukrainian Pronunciation: ukra-jina), derived from its etymology, describes the borderlands between the Kyivan Rus' and Poland. This historical name dating back to the 12th century aptly describes in the modern context a nation that stands as the border between the Russian Federation and the West. The victim of a sustained grey zone conflict since 2014, Ukraine is a case study of both hybrid conflict and the evolution of national informational and cyber conflict between a regional power and a medium-sized weak state. Ukraine's experiences highlight the challenges associated with what is best referred to as a cybered conflict fostered by a new era of socio-technical uncertainty and insecurity. This chapter examines the reality of cybered conflict generated by socio-technical uncertainty originating out of information warfare and cyberattacks between two nations and serves as a testing bed of multiple theories and concepts on deterrence, norms, and security developed over the last 30 years.

Ukraine has been under sustained assault in and through cyberspace both prior to and following the collapse of the Yanukovych regime on February 22, 2014. How Ukraine has addressed the assault on its sovereignty in cyberspace and beyond has been the subject of multiple works on hybrid warfare. Yet few of these works have examined how Ukraine specifically addressed its challenges. Ukraine's approach to cyber and information warfare following the Revolution of Dignity (Euromaidan) serves as a robust case in how to confront a larger aggressive adversary in cyberspace. Ukraine's approach to national cyber security and information security is a work in progress highlighting the challenges of developing organizational structures within contentious political and social environments.

Information warfare and cyberattacks against Ukraine constituting socio-technical assaults occurred in tandem with political fragmentation and reorganization in the face of adversarial activities. Russian news organizations and social media such as Odnaklassniki and Vkontakte rapidly disseminated a narrative of events counter to the perceived realities taking place during Ukraine's Revolution of Dignity (Frum 2014). Beyond sustained information operations, protesters were also subject to a variety of cyberattacks including DDoS[1] and SS7[2] attacks. Attacks on mobile infrastructures targeted the protesters with SMS messages ominously warning "Dear subscriber, you are registered as a participant in a mass disturbance" (Hooton 2014). This form of attack would become prevalent in the

DOI: 10.4324/9781003110224-13

months following Euromaidan and Ukrainian soldiers and their families would be increasingly targeted with similar attacks (Brantly, Cal, and Winkelstein 2017a). Other cyberattacks, mainly DDoS, against opposition websites and protest infrastructures were also common (Pakharenko 2015).

These initial information and cyber operations would become part of a larger and arguably more complicated informational and cyber security environment in the months and years following Euromaidan. Extending well beyond the Ukrainians engaged along a physical contact line with Russian soldiers and their proxies in the East of Ukraine, Ukrainian citizens across the nation have felt the impact of sustained information and cyber operations. These sustained operations create a perpetual siege mentality (Brantly et al. 2017b).

This chapter deconstructs the bureaucratic politics of the state and examines the actions Ukraine has undertaken to address Russian information operations and cyber warfare. Combined, these constitute a change in how Ukrainians address and understand information operations and cyber security. This chapter proceeds in four sections. The first section examines the state of the bureaucracy of Ukraine as it related to information operations and cyber security at the time of the collapse of the Yanukovych government. The second section examines the efforts of Ukraine and her citizens to address information and cyber security challenges. The third section discusses the process of changing the fundamental approach to national cyber and information security in Ukraine. Finally, the chapter concludes with a discussion on the future of Ukrainian approaches to national information and cyber security.

Bureaucratic bits and bytes

Ukraine's woes in cyberspace and information warfare are not solely attributable to external factors. Ukraine's domestic political structures, unitary government, rigid and often ineffectual bureaucracy, and what Paul D'Anieri (2006) refers to as a state of "rule by law rather than rule of law" exacerbate external interventions into the nation and impede efficient responses and the development of effective institutions capable of safeguarding Ukraine. At its most basic, Ukraine is challenged by a consolidation of power within its bureaucracy. This consolidation returns Ukraine to a highly centralized bureaucracy with traditionally embedded criminal–political interests and high levels of corruption. This leads to a situation in which laws are drafted, passed, and institutions are created and staffed but the application of law is inconsistently applied (due to criminal or corruption interests), and institutions are unable to operate effectively without highly centralized control.

Prior to the Revolution of Dignity, Ukraine had a bevy of more than 22 laws on the books associated with information and cyber security. The number and extent of legislation on cyber security and information security in Ukraine prior to 2014 might lead outside observers to believe Ukraine had an effective information security apparatus in advance of Euromaidan. Prior to legislating information and cyber security, the Ukrainian government established, as far back as

1991, the State Special Communications Service of Ukraine (Державна служба спеціального зв'язку та захисту інформації України) and in 2007 established a computer emergency response team (CERT-UA) ("CERT-UA: скорая киберп омощь – PC Week/UE" 2014). Despite all the above laws the state of cyber and information security in Ukraine at the time of Euromaidan was weak. The laws in aggregate deal with many of the conventional challenges associated with information and cyber security.

Despite the robustness and conscientious nature of the laws on the books, the actual enforcement of these laws was subjective at best (D'Anieri 2006). The selective enforcement of legal regimes is in line with highly consolidated power structures. D'Anieri (2006) notes that the consolidation of power does not make the laws inapplicable but creates the conditions under which their application is subject to the discretion of those in political power rather than decentralized administration based on a robust jurisprudence. Taras Kuzio (2015) notes that that the consolidation of power leads to challenges associated with endemic corruption among and within political parties that privileges the interests of an oligarch class. Ukrainian corruption forms a powerful criminal–political nexus of rent-seeking, rent disbursements, and large patronage networks (Kudelia and Kuzio 2015). This criminal–political nexus discourages inconsistencies within political party development and fosters a centralized approach within the frameworks established by party leaders.

Centralized administration limits the autonomy of various state organs. Concurrently, the need to distribute rents associated with a centralization of power and the creation of patronage networks necessitates the construction of a large bureaucracy. In Ukraine during the Yuschenko era the inability to form coalitions or stable governing factions within the Verkovna Rada created a situation in which laws and regulations were on the books but a lack of centralized authority limited their impact. Yet, following the 2010 election and return of Viktor Yanukovych to power, the political structures which under the Yuschenko period were forced to devolve presidential power to the parliament and the prime minister were reversed (Sedelius and Berglund 2016). However, because of the need to maintain patronage and rents the incentive to universally apply legal standards was absent and therefore resulted in an imbalanced and weak utilization of existing legal structures.

Despite having laws on the books, there appears to have been limited enforcement or selective enforcement. Moreover, any resort to prosecution was also likely undermined by substantial penetration by foreign "partners" and a lack of capacity and will within the organs of state to enforce already approved laws. Some reports indicate that under the Yanukovych government Ukrainian security services were penetrated substantially, with up to 30% of the SBU officers being from the FSB (Russia's Security Service) (Galeotti 2014). The foreign officers within the domestic intelligence and security services of Ukraine (FSB) were not solely there due to good case work by Russian FSB officers, rather they were there through a 2010 "cooperation protocol" that explicitly allowed Russian agents in the Ukrainian security services (Galeotti 2014).

The lead-up to Euromaidan Ukraine experienced a shifting media landscape that made accurate, balanced information a rare commodity. As noted by Sergii Leschenko (2014), despite passage of access-to-information legislation, the law was incomplete, never fully implemented and often circumvented on flawed pretenses. This was problematic in a state in which most citizens receive their news through the television (90%) (International Republican Institute 2014), the print news sector is underdeveloped and the major media concerns were controlled by the existing political power brokers including the president. Beyond the challenges associated with a constrained media environment domestically and insufficient legal standards to provide information to the public, almost one-third (30%) of Ukrainians according to a research by the International Republican Institute received their news from Russian media (IRI *Public Opinion Survey Residents of Ukraine* 2014).

To circumvent the controlled media environment online news became increasingly popular. Yet, as the shift away from controlled sources of media occurred, DDoS attacks and false domain attacks on news websites increased (Leshchenko 2014). Glib Pakharenko (2015), in analyzing the increasing number of cyberattacks during the early days of the revolution, noted a distinct cybercriminal nexus and a variety of types of malware directed at everything from social media accounts and websites to phones and financial activities. Pakharenko (2015) also commented on the diversity of IP addresses being used to target Ukrainians during the Euromaidan.

Prior to the overthrow of the Yanukovych regime, Ukraine's cyber and information environments were primed for substantial interference both bureaucratically, with a highly consolidated corrupt, rent-seeking regime that failed to enforce or selectively enforced laws, and an established governance structure in which the institutions tasked with enforcing laws were beholden to political higher-ups. A highly consolidated mass media market with extensive governmental concerns and large foreign presence challenged limited information validity. When Euromaidan began, Facebook and Twitter were not the most popular social networking sites, instead Russian owned Vkontakte and Odnokassniki were. At the basic technical level, Ukraine was heavily dependent on Russian network and information interception capabilities known as SORM[3] and the mobile, terrestrial, and orbital communications firms were owned in part or entirely by entities within the Russian Federation and transnational organized cybercrime organizations (Soldatov and Borogan 2015).

Countering propaganda and disinformation – a hybrid approach

Following the revolution, Ukraine was in political and bureaucratic disarray. The SBU, the state internal security service, experienced major personnel upheavals and its former head was the subject of an extradition request (Interfax 2015) and reports of significant Russian intelligence penetrations were rampant (Miller 2014b). After Euromaidan, more than 325 SBU officers had been removed and

25 had been charged with treason and all regional directors had been replaced (Miller 2014b).

Beyond the SBU, major personnel changes took place across nearly all government ministries. Systemic underfunding of the defense sector combined with rampant corruption set the post-revolutionary status of the military in a perilous position (Oliker et al. 2016). By 2014 out of Ukraine's total military force of 129,950, only 6,000 troops were combat ready and able to counter Russian intentions in Crimea and in Eastern Ukraine (Brantly, Cal, and Winkelstein 2017a). Every organization under the control of Ukraine's National Security and Defense Council (NSDC) was impacted by the change in governance.

The re-establishment of functional governance began when the political controls which fostered a consolidation of power and the existing rent-seeking and distribution networks that left decisions isolated to those at the top of the political hierarchy collapsed. The power vacuum in Ukraine left a large number of mid-tier bureaucrats and the existing bureaucratic culture in place while the temporary government and subsequently the new administration of Petro Poroshenko appointed new leadership to replace the old (Ash et al. 2017). Just as elsewhere, bureaucratic cultures in Ukraine, once entrenched, make change extremely difficult (Wilson 1989). Re-establishing the centralized bureaucracy while possible was challenged organizationally and functionally, as the social norms and practices of state governance developed under the previous government were being rebuilt.

While the Ukrainian leadership was new, change in addressing issues related to cyber security and information security were slow and bogged down in conventional inter-ministry bureaucratic relations that heavily resemble political or bureaucratic fragmentation. The status quo prevailed at the functional level of government. Because of ongoing crises in Crimea and in Eastern Ukraine, little thought was given to unfolding cyber and information warfare activities. Moreover, the new government, in particular nationalist MPs within the Verkovna Rada, failed to grasp the extent of Russian information interference and the impact that their post-revolutionary actions might have on the continuing Ukrainian crisis when they proposed eliminating the status afforded to the Russian language (Kudriavtseva 2016). Although the law never made it past the president, the advancement of a single language, Ukrainian, under the guise of national identity consolidation and security provided substantial fodder for Russian propaganda and information warfare efforts.

After the revolution Ukraine increasingly suffered sustained information operations and limited cyber operations. The pernicious nature of Russian propaganda indicated strong effects with upwards of 80% of the population of the Donbas believing the narrative that Euromaidan was organized by Ukrainian nationalists with substantial assistance from the United States (Kudriavtseva 2016). The impact of propaganda targeted at the Eastern Oblasts was four times as impactful as the same propaganda directed against Western Oblasts (Kudriavtseva 2016). These information campaigns sought to systematically undermine the social and political fabric of the Ukrainian state. These information operations

were socio-technical in nature and sought to exploit historical, cultural, linguistic, regional, and religious tensions and grievances via universal technical platforms.

One particularly egregious example of information warfare occurred when a Buk missile (surface-to-air missile) was fired from rebel-held territories in Eastern Ukraine (Toler 2014). The violence of the attack was matched by Russian attempts to seek to pin the blame for the attack on Ukraine (Fitzgerald and Brantly 2017). Eventually BellingCat (2017), an independent investigative journalism organization, provided substantial evidence including photographs and videos of the Buk missile system in rebel-held territories both before and after the attack (missing a missile). A Dutch criminal investigation completed four years later came to the same conclusion.

In May 2017 President Poroshenko, in the face of continued information operations, by presidential decree blocked access to a variety of Russian social media, news, and other technology sites (Freedom House 2017). Every individual or organization I met with while in Ukraine had nearly the same response: "we are under attack; we must protect the nation". Ukrainian academics acknowledged the poor precedent the decree established with regard to the freedom of speech, yet they each in turn commented on the absolute necessity of the implementation. From the time of election until May 2017 Ukraine had no formal decree or legislation to combat information warfare directed against it.

Despite a lack of formal legislation or decrees on information warfare, the Ukrainian government was not passive. Hundreds of signs, television programs, radio programs, and other popular propagandist platforms were being implemented and used nationwide. Many of the signs in Metro stations and around the country encouraged individuals to speak Ukrainian, to take pride in being Ukrainian. Simultaneously, generally positive support, through Facebook groups, civil society organizations, and a variety of newly established NGOs sought to promote national identity and recognition. These efforts were critical in the early months of the Eastern conflict as Ukrainian soldiers and volunteer battalions engaged in sustained conflict operations with limited supply lines and little to no medical assistance (Marten and Oliker 2017).

Information operations were not limited to broad societally based attacks; some of the most aggressive attacks sought to undermine the psychological capacities of the soldiers and their families increasingly engaged in both regular and volunteer units in Ukraine. Information operations on the front lines included SS7 attacks, the use of android hijacking software, the penetration of wireless and fixed line information infrastructures, and other targeted information attacks (Brantly et al. 2017a). Very early in the conflict Russian signals intelligence equipment was placed near the contact line between Ukrainian and separatist forces. Members of the Information Assurance Directorate as well as enlisted personnel from both volunteer and regular Ukrainian battalions engaged on the contact line provided evidence of targeted information operations.

To date the overwhelming response of Ukraine to information warfare has emphasized three distinct categories and styles of approach. First, several organizations engaged in processes of identification and correction of information

operations through organizations such as StopFake.org and InformNapalm.org and others. Ukrainian and foreign journalists indicate these platforms offer a means of informed counter information warfare using facts and logic.

Second, a variety of government initiatives both legislated and by decree have been undertaken in Ukraine to both foster resilience and combat information warfare. In December 2014 the Verkhovna Rada of Ukraine established the Ministry of Information Policy (MIP) (Matychak 2017). Article 1 of the general provisions of the MIP states: "The Concept purpose is to ensure information sovereignty and determination of approaches to protection and development of national information space for comprehensive information support of Ukrainian society".[4] The creation of the MIP raised concerns that it might transform into an Orwellian information ministry controlling and regulating free speech (Miller 2014a). The MIP was designed to work with journalists, foster national media literacy, emphasize counter information operations in the Anti-Terrorist Operation Zone (ATO), and carry out social media campaigns. The MIP has partnered with NGOs and developed a project, funded by the European Endowment for Democracy Foundation to fund an Open Source Intelligence (OSINT) academy that developed digital courses on information verification (Matychak 2017). The efforts of the MIP have been moderately successful but it lacks funding and suffers from potential reputational challenges.

The Ukrainian government by presidential decree has not only closed access to various web platforms, it has also selectively enforced legal statutes on transfrontier advertising to shutter Russian broadcast channels. Moreover, Ukraine has also banned some journalists from legally entering the country. Each of these restrictive moves and the introduction of the MIP has raised substantial concerns within the human rights and free speech communities internationally. In Ukraine, however, many see these moves as necessary to safeguard Ukraine against foreign interference.

Part propaganda, part counter information operation, the Ukrainian Ministry of Defense has consistently for the better part of the last four years managed to distribute on a near daily basis maps indicating their assessment of the status of forces along the ATO zone and violations of the Minsk agreements signed between the belligerents. These information operations combined with troop resilience trainings have hardened Ukrainian forces against various forms of information operations.

Third, both domestic civil society NGOs independently and with the aid of foreign governments and IGOs have developed a series of initiatives. One of the most famous of these is the Ukraine World Project sponsored by the European Union, International Renaissance Foundation, Civic Synergy, the Ukrainian government, Open Society Foundation, and Internews.[5] Other organizations such as the Ukraine Crisis Media Center, the OSCE Euromaidan Press and a variety of others have created a variety of engagement platforms to continue to challenge propaganda and disinformation in Ukraine, train civil society and journalists, and provide advice to policymakers. All of these organizations form a counter information operations cacophony that was nonexistent in 2013 and early 2014. While

Ukraine is still susceptible to information operations, its resilience has increased markedly.

Although many of the initiatives undertaken by Ukraine and partners have improved, the status of information balance between the two parties means they face several challenges endemic to a country challenged by corruption and consolidation of power and economic weakness. Concerns about information manipulation in Ukraine are well-founded and recently arose around concerns that the government was manipulating corruption commission reporting and hiding information when it stripped former Georgian President and Former Governor of Odessa Oblast Mikhail Saakashvili of his Ukrainian citizenship and arrested him (Karatnycky 2018). Beyond the challenge of preventing abuses of power by the state in utilizing information operations is a concern about the potential loss of funding from any of the many outside organizations currently financing and providing support to Ukrainian organizations. The successes of counter information and propaganda operations in Ukraine are in large part due to the involvement of the international community and the engagement of civil society, academia, and journalists. These engagements provided a capability that extended beyond the state minimized but did not eliminate the challenges associated with power consolidations and endemic bureaucratic cultures in Ukraine.

The approach to information warfare in Ukraine has been diverse with both bottom-up and top-down developments. Many of the most successful elements of Ukrainian counter information operations have been organic, evolved from civil society or within academia. The story of Ukraine's efforts to counter cyber operations followed a different trajectory.

Addressing Ukrainian cyber security challenges – A centralized approach

Whereas the information warfare situation in Ukraine has been addressed by both decentralized non-governmental and centralized governmental approaches, the cyber conflict in Ukraine has primarily been confined to state bureaucracies. Ukraine has historically been a hotbed of global cybercrime despite its affirmation of the Budapest Convention on Cybercrime and laws on its books dealing with cybercrime (Kostyuk 2015). Ukraine's endogenous cyber capacity is remarkably high. Ukraine produces excellent students with computer science and engineering backgrounds but suffers immensely from economic challenges and a poor political and a burdensome business regulatory environment. Many cyber activities in Ukraine take place under a perception, rooted in social norms, that cybercrime directed against non-Ukrainians constitutes hooliganism rather than a "serious" crime (Kostyuk 2015).[6] Throughout the 1990s and 2000s Ukraine was designated a priority foreign country for its substantial violations of intellectual property rights (IPR) (USTR 2001). Ukraine's adherence to IPR was so poor, that it was sanctioned in the early 2000s and was threatened with denial of its World Trade Organization aspirations if it did not implement reforms (Grassley 2005).

Ukrainian IPR failures might seem an odd starting point, but as of the late 2000s the most common forms of operating systems and software used on devices in Ukraine came from bootleg markets such as Kyiv's famous Petrivka Market. An aging soviet infrastructure, penetrated intelligence services, firms owned in part by Russian interests, and a variety of other market and criminal concerns left Ukraine exposed to potential cyber exploitations. Cyber exploitations came in droves and continue to persist five years after initial hostilities (Baezner and Robin 2017). Over the period of March 2014–June 2018, Ukraine has been the site of some of the most significant cyberattacks ever perpetrated. As noted by Wired reporter Andy Greenberg (2017), Ukraine became the equivalent of a test lab for Russian cyber capabilities. The impact of these attacks was substantial in monetary, reputational, and in the case of attacks against Ukrainian soldiers potentially lives. These attacks impacted access to systems, slowed transport, and reduced or halted services. The attacks are continuous and escalating in both breadth and severity. Actors involved in the perpetration of attacks against Ukraine have been tied through various technical and non-technical analyses to elements of the FSB, GRU, non-state, and criminal groups (ICS-Cert 2016; Zetter 2016; Greenberg 2018).

Ukrainian cyber defense responsibilities reside within the NSDC and encompass the Ministry of Defense (MoD), the Security Service of Ukraine (SBU), Ministry of Internal Affairs (MIA), the Ukrainian Intelligence Community (UIC), and the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) (Kostyuk 2015). In 2017 the coordinating entities of the NSDC related to cyber were managed by a single individual reporting to the NSDC Chairman. In 2017 the NSDC's cyber components were severely understaffed, suffered from personnel turnover, or simply lacked funding to undertake their stated mission.

Ukraine's first cyber security strategy approved by presidential decree and released in 2016 included an acknowledgment that Ukraine's cyber infrastructure has been attacked and that the establishment of a formal cyber security system emphasizing countering cyberterrorism, protection of critical infrastructures, including the military, energy, transportation, and banking spheres, was necessary (Office of the President of Ukraine 2016). The document outlined and proposed that the state would work with NATO and EU members to establish "best practices" within Slightly more than two years after the ousting of the Yanukovych government and following more than 50 severe cyberattacks including those perpetrated against Ukrainian electric infrastructure, Ukraine had a working cyber strategy. The 2-year delay between change of administration and the establishment of a strategy constituted a monumental shift in the bureaucratic and functional approaches to national cyber security in Ukraine. The reorganization codified through presidential decree the organizational structure of cyber defense under the NSDC.

As of 2017 the NSDC Cybersecurity Coordination Center Ukraine followed a legal pathway originating in the constitution of Ukraine, and proceeding through the Law on the National Security of Ukraine (2003, Revised June 21, 2018),

the National Security Strategy of Ukraine (2015), the Cybersecurity Strategy of Ukraine (2016), and subsequent annual plans of Cybersecurity Strategy implementation. Ukrainian cyber security was further codified in the October 2017 law on national cyber security. Legally, strategically (based on strategy documents), Ukraine moved very quickly. Yet despite all the improvements it made on paper, its bureaucracy in 2014 was ill-equipped both organizationally and functionally to deal with the challenges it faced.

Ukraine faces significant challenges: First, financial challenges remain a persistent and insurmountable roadblock to the retention of individuals within the military, SSSCIP CERT-UA, police forces, and most other official government positions. Financial remuneration for frontline soldiers and personnel in all of the organizations listed is not competitive with general national nor global market forces. Although this problem is not confined to Ukraine (Wenger et al. 2017), conversations with principles and subordinates indicated extreme pay disparities between individuals in the public sector and those in the private sector. Overall, government service wages constitute a significant matter of concern for Ukrainian security sector reform (Oliker et al. 2016).

Ukraine continues to receive international support for a variety of training initiatives. The United States, NATO and various EU countries, the OSCE, and others provided funding for material resources, the establishment of training centers, equipment for defensive cyber operations, training for police and CERTS, and a variety of affiliated projects (Seals 2017). More than US$1.7 million dollars was committed to Ukraine for cyber defenses by NATO countries (NATO 2016). The United States has sent national guard Units to Ukraine to engage in cyber security training missions. Despite repeated training of Ukrainian military and civilian cyber defense personnel the infrastructure to retain these persons within government service is lacking. Internal documents and conversations with the General Staff of Ukraine indicate that the military services have the most significant retention problem.

Second, although Ukraine lacks the necessary financial resources required for the development and maintenance of cyber defense, the more serious challenge of bureaucratic cultures undermines the ability of Ukraine to systematically establish balanced cyber defenses. All indications both in public and private conversations highlighted the disproportionate control of cyber defense within the SBU.

Despite the bureaucratic challenges, there are some positive changes bureaucratically and financially. Ukraine is presently participating in international training activities such as NATO's Cooperative Cyber Defence Centre of Excellence exercise Locked Shields and even won the 2017 competition (Zilberman and Logan 2018). Each new attack is often followed by a period of increased financial and technical support from European, US, and NATO allies (Paganini 2017). Yet, despite increasing external support, the status quo of cyber security in Ukraine remains inadequate (Williams 2017). Efforts to appropriately distribute resources do appear to be achieving some success, particularly in areas of critical infrastructure (Reuters 2018).

From largely ineffectual beginnings in 2014 until Fall 2018 Ukraine had undergone immense legal and organizational changes. It has revised its national security strategy to include cyber security; it has reorganized and established cyber as a core component of the NSDC. It has written and approved a national cyber security strategy and it recently passed national cyber security legislation. Ukraine has accomplished all of these changes in under four years. Organizationally it has established a rubric for success, but this rubric is still challenged by existing bureaucratic cultures and economic challenges.

Conclusion: Ukrainian cyber and information security in the present and future

Ukraine's bureaucratic cultures are evolving and there have been substantial roadblocks within certain organizations and by certain political figures, but what Ukraine has accomplished over a period of four years, with external help from foreign states, international organizations, and nonprofit assistance has been substantial. It is hard to over-state the challenges Ukraine faced in 2014 and how far it has come. Its approaches to national information security and national cyber security have taken markedly different paths and have achieved fundamentally different outcomes. Ukraine still suffers under sustained information warfare and from cyberattacks. It is growing increasingly resilient to information warfare, yet these same improvements are not carrying over to cyberattacks.

Information security and cyber security require different infrastructural and organizational capabilities. The hybrid development of information resilience through the creation of the Ministry of Information Policy and more importantly through the engagement of civil society to address the challenge of information warfare has proven successful. Fewer capital resources – human and physical – were necessary to achieve resilience in the information space. The sustainment of information warfare resilience is also likely self-perpetuating in ways that cyber security is not. As concepts of national pride and identity, laws on the prevention of disinformation and propaganda come into force, the population of Ukraine is likely to increase rather than decrease its resilience to outside manipulations.

The development of cyber security structures in Ukraine, by contrast, has been highly centralized. The organizations that gained responsibility for cyber security in Ukraine were already in existence prior to 2014 (with the exception of the national cyber police). They each had embedded cultures and relationships within the NSDC and the power structures of Ukraine. Each of these organizations was already familiar with the limited resource environment and generally unable to circumvent it. The laws and processes established look good on paper. They align with European and NATO standards, but they are akin to bolting on new organizational structures and goals to existing frameworks. There are motivated individuals within each of the organizations. Each organization expressed a strong and genuine interest to address cyber security concerns, yet each organization, by necessity had many other priorities that often-superseded cyber security.

The Ukraine case serves as the canary in the coal mine. The likelihood that information operations and cyber operations will become commonplace in conflict is almost assured. Assessing how states under duress address challenges when they are at their most vulnerable provides valuable insights that might hopefully mitigate similar issues in future situations faced by a range of states. Few countries have been so strenuously tested in the information space and in cyberspace as Ukraine. And few countries could reasonably have been expected to reorganize and establish laws and strategies as quickly as Ukraine has. It has done so with external assistance in many cases, but also through a new-found ability to coordinate and work across ministries and divisions of government. Yet, issues of patronage and rent-seeking and rent distribution remain high and often stifle the innovation and aspirations of mid-level bureaucrats. Political and bureaucratic fragmentation, in addition to all the external challenges imposed upon the state by the Russian Federation, remain clear roadblocks to instituting sustained and meaningful reform. If Ukraine is to improve its resilience in cyberspace, commensurate with its advances in resilience to information warfare, it must necessarily address the core issues of financial allocations within the NSDC and the coordination and consolidation of power within certain ministries. Absent a sustained ability to fund the front lines of cyber defense in Ukraine strategy, law and organizational developments will be insufficient to maintain the human capital required for national cyber security. Finally, if Ukraine is unable to foster coordination and cooperation amongst the various NSDC entities then duplication of effort, interagency animosities, and inadequate cyber security outcomes are likely.

Notes

1 Distributed Denial of Service.
2 An SS7 attack is an exploit that takes advantage of a weakness in the design of SS7 (Signaling System 7) to enable data theft, eavesdropping, text interception, and location tracking.
3 SORM – System for Operative Investigative Activities (Система оперативно-разыскных мероприятий,).
4 https://mip.gov.ua/files/documents/Concept.docx
5 http://ukraineworld.org/infowars/
6 These factors were also identified repeatedly in discussions at Kyiv Polytechnic National University and with members of the defense industrial base.

References

All links checked on August 23, 2021.

Ash, T., Gunn, J., Lough, J., Lutsevych, O., Nixey, J., Sherr, J., and Wolczuk, K. (2017). *The Struggle for Ukraine*. London: The Royal Institute of International Affairs.

Baezner, M., and Robin, P. (2017). *CSS CYBER DEFENSE PROJECT Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict*. Zurich: Center for Security Studies (CSS). Retrieved from: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pdf.

BellingCat. (2017). MH17 - The Open Source Investigation Three Years Later. Retrieved from: https://www.bellingcat.com/wp-content/uploads/2017/07/mh17-3rd-anniversary-report.pdf.

Brantly, A. F., Cal, N. M., and Winkelstein, D. P. (2017a). *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW*. West Point, NY: U.S. Army Cyber Institute. Retrieved from: https://apps.dtic.mil/sti/pdfs/AD1046052.pdf.

Brantly, A. F., Cal, N. M., and Winkelstein, D. P. (2017b). Don't Ignore Ukraine: Lessons from the Borderland of the Internet. Retrieved from: https://www.lawfareblog.com/dont-ignore-ukraine-lessons-borderland-internet.

CERT-UA. (2014, October 16). скорая киберпомощь. PC Week/UE. Retrieved from: http://www.pcweek.ua/themes/detail.php?ID=147850.

Office of the President of Ukraine (2016) Cybersecurity Strategy of Ukraine. Retrieved from: https://ccdcoe.org/uploads/2018/10/NationalCyberSecurityStrategy_Ukraine.pdf

D'Anieri, P. (2006). *Understanding Ukrainian Politics*. London: M.E. Sharpe.

Fitzgerald, C. W., and Brantly, A. F. (2017). Subverting Reality: The Role of Propaganda in 21st Century Intelligence. *International Journal of Intelligence and Counter-Intelligence*, 30(2): 215–240. https://doi.org/10.1080/08850607.2017.1263528.

Freedom House. (2017). *Ukraine Country Report | Freedom on the Net 2017*. Washington, DC: Freedom House. Retrieved from: https://freedomhouse.org/report/freedom-net/2017/ukraine.

Frum, D. (2014, March 26). Ukraine's Phantom Neo-Nazi Menace. *The Atlantic*. Retrieved from: https://www.theatlantic.com/international/archive/2014/03/ukraines-phantom-neo-nazi-menace/359650/.

Galeotti, M. (2014, October 30). Moscow's Spy Game. *Foreign Affairs*. Retrieved from: https://www.foreignaffairs.com/articles/russia-fsu/2014-10-30/moscows-spy-game.

Grassley, C. (2005, November 18). Grassley Praises Senate Passage of Jackson-Vanik Repeal for Ukraine. United States Senate Committee on Finance. Retrieved from: https://www.finance.senate.gov/chairmans-news/grassley-praises-senate-passage-of-jackson-vanik-repeal-for-ukraine.

Greenberg, A. (2017, June 20). How an Entire Nation became Russia's Test Lab for Cyberwar. *Wired*. Retrieved from: https://www.wired.com/story/russian-hackers-attack-ukraine/.

Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. Retrieved from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hooton, C. (2014, January 22). Ukraine Protests Demonstrators in Kiev Received Disturbing Mass Text. *Independent*. Retrieved from: https://www.independent.co.uk/news/world/europe/ukraine-protests-demonstrators-in-kiev-receive-disturbing-mass-text-9077327.html.

ICS-Cert, NCCIC. (2016, March 7). IR-ALERT-H-16-043-01BP Cyber-Attack against Ukrainian Critical Infrastructure, 1–17. Retrieved from: https://www.eenews.net/assets/2016/07/19/document_ew_02.pdf.

Interfax. (2015, January 12). Ukraine Accuses Russia of Breaking CIS Agreements over Yanukovych Extradition. Retrieved from: https://en.interfax.com.ua/news/general/243934.html.

International Republican Institute. (2014, April 4) *Public Opinion Survey Residents of Ukraine*. Washington, DC: International Republican Institute.

Karatnycky, A. (2018, February 12). The Rise and Fall of Mikheil Saakashvili. *Politico*. Retrieved from: https://www.politico.eu/article/the-rise-and-fall-of-mikheil-saakashvili/.

Kostyuk, N. (2015). Ukraine: A Cyber Safe Haven? In K. Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, pp. 113–122.

Kudelia, S., and Kuzio, T. (2015). Nothing Personal: Explaining the Rise and Decline of Political Machines in Ukraine. *Post-Soviet Affairs*, 31(3): 250–278.

Kudriavtseva, N. (2016). Ukraine: What's a Language for? *Kennan Cable*, 15: 1–9.

Kuzio, T. (2015). *Ukraine, Democratization, Corruption and the New Russian Imperialism*. Santa Barbara, CA: Praeger Security International.

Leshchenko, S. (2014). The Media's Role. *Journal of Democracy*, 25(3): 52–57.

Marten, K., and Oliker, O. (2017, September 14). Ukraine's Volunteer Militias May Have Saved the Country, But Now They Threaten It. *War on the Rocks*. Retrieved from: https://warontherocks.com/2017/09/ukraines-volunteer-militias-may-have-saved-the-country-but-now-they-threaten-it/.

Matychak, T. (2017). David against Goliath: How Ukraine Resists the Kremlin's Information Attacks. In A. Kulakov (ed.), *In Words and Wars: Ukraine Facing Kremlin Propaganda*. Kyiv: Internews-Ukraine.

Miller, C. (2014a, December 2). Ukraine Just Created Its Own Version of Orwell's 'Ministry of Truth'. *Mashable*. Retrieved from: https://mashable.com/2014/12/02/ukraine-ministry-of-truth/#AKpasiKpEOq9.

Miller, C. (2014b, December 30). Ukraine's Top Intelligence Agency Deeply Infiltrated by Russian Spies. *Mashable*. Retrieved from: https://mashable.com/2014/12/30/russian-vs-ukrainian-spies/#y6rqmk6rUOq3.

NATO. (2016, June). *Ukraine Cyber Defence*. Brussels: NATO.

Oliker, O., Davis, L. E., Crane, K., Radin, A., Gventer, C. W., Sondergaard, S., Quinlivan, J. T., Seabrook, S. B., Bellasio, J., Frederick, B., Bega, A., and Hlavka, J. (2016). Security Sector Reform in Ukraine. RAND Corporation. Retrieved from: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1475-1/RAND_RR1475-1.pdf.

Paganini, P. (2017, July 12). Following NotPetya NATO Increases Support for Ukraine's Cyber Defenses. *Security Affairs*. Retrieved from: https://securityaffairs.co/wordpress/60941/cyber-warfare-2/nato-support-ukraine-cyber security.html.

Pakharenko, G. (2015). Cyber Operations at Maidan: A First-Hand Account. In K. Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Reuters. (2018, February 6). Ukraine Power Distributor Plans Cyber Defense System for $20 Million. *Reuters*. Retrieved from: https://www.reuters.com/article/us-ukraine-cyber-ukrenergo/ukraine-power-distributor-plans-cyber-defense-system-for-20-million-idUSKBN1FQ1TD.

Seals, T. (2017, February 2). US Army Funds Cyber-Center for Ukraine Military. *Infosecurity Magazine*. Retrieved from: https://www.infosecurity-magazine.com/news/us-army-funds-cybercenter-for/.

Sedelius, T., and Berglund, S. (2016). Towards Presidential Rule in Ukraine: Hybrid Regime Dynamics under Semi-Presidentialism. *Baltic Journal of Law & Politics*, 5(1): 219–27.

Soldatov, A., and Borogan, I. (2015). *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*. New York: Public Affairs.

Toler, A. (2014, November 15). Kremlin Has Mastered Propaganda, but not Photoshop: Fake MH17 Photo Lights Up RuNet. *Global Voices Online*. Retrieved from: https://globalvoices.org/2014/11/15/russia-photoshop-kremlin-mh17-ukraine-crash/.

United States Trade Representative. (2001, March 13). USTR - Ukraine Designated as Priority Foreign Country under Special 301. Retrieved from: https://ustr.gov/archive/Document_Library/Press_Releases/2001/March/Ukraine_Designated_as_Priority_Foreign_Country_Under_Special_301.html.

Wenger, J. W., Oconnell, C., and Lytell, M. C. (2017). Retaining the Army's Cyber Expertise. RAND Corporation. Retrieved from: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1978/RAND_RR1978.pdf.

Williams, M. (2017, August 1). Ukraine Finally Battens Down Its Leaky Cyber Hatches after Attacks. *Reuters*. Retrieved from: https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN1AH35A.

Wilson, J. Q. (1989). *Bureaucracy: What Government Agencies Do and Why They Do IT*. New York: Basic Books.

Zetter, K. (2016, March 3). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired*. Retrieved from: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zilberman, B., and Logan, T. (2018). Increasing U.S.-Ukraine Cyber Cooperation is a Step in the Right Direction. Foundation for the Defense of Democracies (blog). Retrieved from: http://www.defenddemocracy.org/media-hit/boris-zilberman-increasing-us-ukraine-cyber-cooperation-is-a-step-in-the-right-direction/.