State of the Art of Cyber security and Cyberconflict Research Conference, 27-29 September 2018, Zürich.

Battling the Bear: Ukraine's Approach to National Cyber and Information Security (DRAFT)

Aaron Brantly, PhD
Department of Political Science
Assistant Professor, Virginia Polytechnic and State University

Abstract:

Ukraine has faced substantial challenges across multiple fronts its successful 2014 Revolution of Dignity. Among the greatest challenges Ukraine has faced is the establishment of a national cybersecurity infrastructure capable of withstanding cyberattacks and information operations against military and civilian infrastructures. Ukraine's experience is counterintuitive to the constant refrain in cyberspace regarding asymmetric advantage. Ukraine has struggled with the help of European and NATO allies to forge multiple organizational structures capable to facilitating national information and cyber defense. This work offers detailed analysis on the construction of national information resilience and cyber capabilities by a medium sized state under duress and coercion from an adversary state by leveraging interviews with and documents from Ukrainian ministers, General Staffs, Security Service personnel, soldiers, journalists, civilians and academics conducted over two years. The result is analysis that informs the underlying notions about small to medium state defenses in relation to well-resourced adversaries.

Ukrainian Responses to Sustained Cyber and Information Operations

Ukraine (Україна, Ukrainian Pronunciation: ukra-jina), derived from its etymology literally 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 sustain 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 cybered conflict. This paper is a case study that examines the reality of cybered conflict between two nations that serves as a testing bed for many of the theories and concepts of deterrence, norms, security, civil and military concepts developed over the last 30 years. The intent of this paper is to provide a foundation for future theoretical developments by providing a robust analysis upon which to build.

Ukraine and her citizens, private sector, government, and military have been under sustained assault in and through cyberspace both prior to and following the collapse of the Yanukovych regime on February 22nd, 2014. How Ukraine has addressed the assault on its sovereignty in cyberspace and beyond has respawned a variety of works on hybrid warfare. Yet few works have systemically approached the fall of the Ukrainian state and its subsequent redevelopment under a new political order in the context of how it has approached cyber and information warfare.

Ukraine's approach to cyber and information warfare following the Revolution of Dignity (Euromaidan) is a case study in how a newly established political regime and an active citizenry can and has quickly reoriented laws and policy related to cyberspace as well as begun the process of developing security mechanisms to confront sustained adversarial activities. Ukraine's approach to national cybersecurity and information security is a work in progress but provides a glimpse into the challenges faced by small and medium states in developing organizational structures within fractious societies imbued with substantial challenges such as corruption, contentious bureaucratic politics, and historical institutional legacies.

Information warfare and cyber-attacks against Ukraine occurred in tandem political developments on the ground. As the initial protestors were turning out in the streets Russian news organizations and social media such as Odnaklassniki and Vkontakte were rapidly disseminating a narrative of events counter to the perceived realities on the ground.[1] Russian propaganda on the events transpiring in Ukraine sought to undermine the initial political demonstrations by simultaneously isolating the protestors by declaring them Nazis and concurrently minimize their impact by indicating they were small and inconsequential in number. Both of these facts turned out to be inaccurate. While it is true that Euromaidan did possess a strong undercurrent of nationalism, it is also true that the nationalism expressed by Ukrainians differs from that of the Nazis.[2] Yet the suggestions of the rise of Nazism warranted clarifications and provided fodder for both international skeptics of the revolution and the basis for subsequent annexation or attempts to commandeer territories within Ukraine. Simultaneously information operations taking place in Russian social media and official news outlets, Ukrainian and Russian persons began engaging in sustained attempts to manipulate information commons such as Wikipedia.

In addition to sustained information operations, protestors were also subject to a variety of cyber-attacks including DDoS and SS7 attacks or the utilization of cellular infrastructures. Attacks on mobile infrastructures targeted the protesters with SMS messages ominously warning "Dear subscriber, you are registered as a participant in a mass disturbance."[3] This form of attack would become increasingly prevalent in the months following Euromaidan and Ukrainian soldiers and their families would be increasingly targeted with similar attacks.[4] Other cyber-attacks, mainly DDoS, against opposition websites and protest infrastructures.[5]

These initial information and cyber operations would become part of a larger and arguably more complicated informational and cybersecurity environment in the months and years following Euromaidan. After the Euromaidan revolution a series of sustained information operations have continuously targeted five core constituencies, Russians, all Ukrainians, Eastern Ukrainians,

---

[1] Frum, David. 2014. "Ukraine's Phantom Neo-Nazi Menace." *The Atlantic*. March 26. https://www.theatlantic.com/international/archive/2014/03/ukraines-phantom-neo-nazi-menace/359650/.

[2] Sakwa, Richard. 2016. *Frontline Ukraine: Crisis in the Borderlands*. London: I.B. Tauris.

[3] Hooton, Christopher. 2014. "'Dear Subscriber, You Are Registered as a Participant in a Mass Disturbance'." *Independent*. January 22. http://www.independent.co.uk/news/world/europe/ukraine-protests-demonstrators-in-kiev-receive-disturbing-mass-text-9077327.html.

[4] Brantly, Aaron F, Nerea M Cal, and Devlin P Winkelstein. 2017. "Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW." West Point, NY: U.S. Army Cyber Institute. http://www.dtic.mil/dtic/tr/fulltext/u2/1046052.pdf.

[5] Pakharenko, Glib. 2015. "Cyber Operations at Maidan: a First-Hand Account." In *Cyber War in Perspective: Russian Aggression Against Ukraine*. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

Crimean citizens and residents of Ukraine, and the International community. In addition to sustained post-revolutionary information operations a wide array of cyber operations focused on all sectors of Ukraine ranging from targeting of military and intelligence services to civilian government, elections, physical infrastructure and businesses in or operating through Ukraine also occurred. Although there are substantial numbers of 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.[6]

The bureaucracy of Ukraine has hindered responses to the challenges faced in its engagements with the Russian Federation across domains. While Ukraine has had laws on the books regarding information, intelligence, national security and more, its legacy and its political turmoil over last decade have hindered its ability to implement meaningful change or leverage the capacities it does possess. This paper deconstructs the bureaucratic politics of the state and examines the challenges Ukraine faced both in the immediate aftermath of the Euromaidan revolution, efforts it has undertaken to address them, and efforts of the International community have undertaken to guide Ukraine forward. Combined these efforts foster a process of bureaucratic change that seeks to shift the processes and cultures in Ukraine related to information operations and cybersecurity. This paper proceeds in four sections. The first section examines the state of the bureaucracy of Ukraine as it related to information operations and cybersecurity 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 cybersecurity challenges. The third section discusses the process of changing the fundamental approach to national cyber and information security in Ukraine. Finally, the work concludes with a discussion on the future of Ukrainian approaches to national information and cyber security.

A brief note on methods

This work is based on primary source field research conducted on fact-finding missions over a period of 3 years including discussions with government officials from all national cybersecurity related ministries within the National Security and Defense Council of Ukraine, members of the Ukrainian business community, academics, active, reserve, and retired soldiers from regular and volunteer Ukrainian Army units, members of the US diplomatic mission to Ukraine, NATO mission to Ukraine, members of the US armed forces, and journalists. All primary sources are indicated by category rather than using individually identifiable information except where individuals provided publicly available published information, documentation, and/or presentations. Additional secondary sources provide further technical and specific attributable accounts of Ukrainian responses to the hybrid and specifically cyber aspects of the conflict. The result is a robust and detailed analysis of what is occurring and has transpired in Ukraine in regard to the development of its cyber and information warfare defense capabilities.

Bureaucratic Bits and Bytes

[6] Brantly, Aaron F, Nerea M Cal, and Devlin P Winkelstein. 2017. "Don't Ignore Ukraine: Lessons From the Borderland of the Internet." *Lawfare*. July 7. https://www.lawfareblog.com/dont-ignore-ukraine-lessons-borderland-internet.

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 refers to as a state of "rule by law rather than rule of law"[7] exacerbate external interventions into the nation and impede efficient responses and the development of effectual institutions capable of safeguarding Ukraine. At its most basic Ukraine is challenged by a consolidation of power within its bureaucracy. 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, and institutions are unable to operate effectively without highly centralized control.

Prior to the revolution of dignity Ukraine had on the books a bevy of laws associated with information and cybersecurity. Table 1 lists many of the laws Ukraine had on the books prior to Euromaidan. Each of these laws in some way touched upon digital information, cybersecurity, cybercrime or other elements of the state relevant to cyberspace and information.

Figure 1: Laws of Ukraine Relating to Information and Cybersecurity Prior to Euromaidan[8]

Transliterated Name	**Date of Adoption**
Information Act	1992
Constitution of Ukraine	1996
Print Media in Ukraine Act	1992
On News Agencies	1995
Television and Radio Act	1996
Telecommunications Act	2003
Protection of Public Morality Act	2003
On the Fundamentals of National Security of Ukraine	2003
Electronic Documents and Electronic Document Interchange Act	2004
Electronic Digital Signature Act	2004
On Amendments to the Law of Ukraine – On Payment systems and Transfers of Money in Ukraine	2004
On Amendments to the Criminal and Criminal Procedural Codes of Ukraine (Concerning liability for computer crimes)	2004
Protection of Information and Telecommunications Systems Act	2005
On the Ratification of the Convention of Cybercrime	2005
On Radio and Television Broadcasting	2006
European Convention on Transfrontier Television (Initiated 2002)	2008
(Amendment) On Ratification of the Convention on Cybercrime	2010
Personal Data Protection Act	2010
Information Act (Revised 1992 Act)	2011
Access to Public Information Act	2011

[7] DAnieri, Paul. 2006. *Understanding Ukrainian Politics*. London: M.E. Sharpe. 50.

[8] Kormych, Borys, The Information Law of Ukraine (April 8, 2018). Available at SSRN: https://ssrn.com/abstract=3158729; Streltsov, Lev. 2017. "The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments." European Journal for Security Research 2 (November). Springer International Publishing: 147–84.

Both the number and extent of legislation on cybersecurity 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).[9] 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 cybersecurity. For instance, the Access to Information Act combined a breadth of law that examines both the rights of citizens to information as well as their rights to the privacy and security of the information about them.[10]

Despite the robustness and conscientious nature of the laws on the books the actual enforcement of these laws was subjective at best.[11] The selective enforcement of legal regimes is in line with highly consolidated power structures. D'Anieri 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.[12] Taras Kuzio notes that that the consolidation of power leads to challenges associated with endemic corruption amongst and within political parties.[13] Ukrainian corruption forms a powerful criminal-political nexus of rent-seeking, rent disbursements and large patronage networks.[14] This criminal-political nexus discourages inconsistencies within political party development and fosters a centralized approach within the frameworks established by party leaders.

The centralized approach to the administration of the state 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.[15] However, because of the need to maintain patronage and rents the incentive to universally apply legal standards was absent and therefore resulted imbalanced and weak utilization of existing legal structures.

---

[9] 2014. "CERT-UA: Скорая Киберпомощь - PC Week/UE." *Pcweek.Ua*. October 16. http://www.pcweek.ua/themes/detail.php?ID=147850.

[10] Закон України «Про доступ до публічної інформації» від 13 січня 2011 р. No 2939-VI // Відомості Верховної Ради України. – 2011. – No 32. – Ст. 314.

[11] D'Anieri. *Understanins Ukrainian Politics*. 11.

[12] Ibid.

[13] Kuzio, Taras. 2015. *Ukraine, Democratization, Corruption and the New Russian Imperialism*. Santa Barbara: Praeger Security International.

[14] Kudelia, Serhiy, and Taras Kuzio. 2015. "Nothing Personal: Explaining the Rise and Decline of Political Machines in Ukraine." *Post-Soviet Affairs* 31 (3). Taylor & Francis: 250–78.

[15] Sedelius, Thomas, and Sten Berglund. 2016. "Towards Presidential Rule in Ukraine: Hybrid Regime Dynamics Under Semi-Presidentialism." *Baltic Journal of Law & Politics* 5 (1): 219–27.

Data indicate that from 2002-2011 400 individuals were arrested for Internet and banking fraud charges in Ukraine but only 8 were convicted.[16] Ukrainian officials during the lead up to the 2013 protests did not fail to recognize the capacity of Ukrainian hackers, in fact Valyentyn Petrov an official of the SBU (Sluzhba Bezpeky Ukrayiny), was quoted in the Kyiv Post as saying "Ukrainian hackers are well-known in the world. Our country is a potential source of cyber threats to other countries."[17] This theme of criminality and the interaction between both official and unofficial organizational and criminal elements within Ukraine did not disappear under the Yanukovych regime and based on interviews with members of various organizations the behavior of hacking outside of Ukraine remains to the present a high-reward, low risk endeavor. In 2010 Paul Ferguson of Trend Micro was quoted in the Kyiv post as saying cybercrime emanating from Ukraine exceeded that of Russia.[18]

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 organ 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).[19] 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.[20]

The lead up to Euromaidan Ukraine experienced a shifting media landscape that made accurate, balanced information a rare commodity. As noted by Sergii Leschenko, despite passage of access-to-information legislation, the law was incomplete, never fully implemented and often circumvented on flawed pretenses.[21] This was problematic in a state in which most citizens receive their news through the television (90%)[22], the print news sector is underdeveloped, and the major media concerns were controlled by the existing political power brokers including the President.[23] 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 research by the International Republican Institute received their news from Russian media.[24]

---

[16] Kshetri, Nir. 2013. "Cybercrimes in the Former Soviet Union and Central and Eastern Europe: Current Status and Key Drivers." *Crime, Law and Social Change* 60 (1): 39–65.
[17] Onyshkiv, Y., & Bondarev, A. (2012). Ukraine thrives as cybercrime haven, March 8, http://www.kyivpost.com/news/nation/detail/123965/.
[18] Onyshkiv, Yuriy. 2012. "Ukraine Thrives as Cybercrime Haven - Mar. 08, 2012." *Kyiv Post*. March 8. https://www.kyivpost.com/article/content/ukraine-politics/ukraine-thrives-as-cybercrime-haven-123965.html.
[19] Galeotti, Mark. 2014. "Moscow's Spy Game." *Foreign Affairs*, October.
[20] Ibid.
[21] Leshchenko, Sergii. 2014. "The Media's Role." *Journal of Democracy* 25 (3): 52–57.
[22] 2014. "Public Opinion Survey Residents of Ukraine." Washington, D.C.: International Republican Institute. http://www.iri.org/sites/default/files/2014%20April%205%20IRI%20Public%20Opinion%20Survey%20of%20Ukraine%2C%20March%2014-26%2C%202014.pdf
[23] Ibid.
[24] 2014. "Public Opinion Survey Residents of Ukraine"

To circumvent the controlled media environment online news became increasingly popular. Yet, as the shift away from controlled sources of media changed shifted so did the ire of the state and resulted in DDoS attacks and false domain attacks on news websites.[25] Glib Pakharenko, in analyzing increasing number of cyber-attacks during the early days of the revolution noted a distinct cyber-criminal nexus and a variety of types of malware directed at everything from social media accounts and websites to phones and financial activities.[26] Pakharenko also commented on the diversity of IP addresses being used to target Ukrainians during Maidan.[27]

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 riven with interdependencies including the systemic use of Russian network and information interception capabilities known as SORM and the mobile, terrestrial and orbital communications firms owned in part or entirely by entities within the Russian Federation and transnational organized cybercrime organizations.[28]

From the outset, Ukraine was behind or worse on cyber and information security examined from every single measure. Politically, bureaucratically, socially and technically information and cyber security in Ukraine required a complete overhaul. This overhaul was to come amidst sustained kinetic conflict and economic disaster. The next 2 sections focus on what organizations and capabilities Ukraine and her citizens have built to foster both information and cybersecurity. The primary concern of each of these parts is an assessment of whether the developments have resulted in improvement on the immediate post-revolution state of affairs.

Countering Propaganda and Disinformation – A Hybrid Approach

To confirm the scope of the challenges in Ukraine one of the first questions asked of civil society organizations was whether they had evidence to confirm the political or bureaucratic disarray present in the immediate aftermath of Euromaidan. The response was that in the aftermath of Euromaidan the central offices of Ukraine's security services in Kyiv were ransacked. Files had been strewn about the floor, desk drawers had been pulled out and computers damaged. The accounts of political and bureaucratic disarray within the SBU align with official court documents

[25] Leshchenko, Sergii. 2014. "The Media's Role." *Journal of Democracy* 25 (3): 52–57.
[26] Pakharenko, Glib. 2015. "Cyber Operations at Maidan: a First-Hand Account." In *Cyber War in Perspective: Russian Aggression Against Ukraine*. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.
[27] Ibid.
[28] Soldatov, Andrei, and I Borogan. 2015. *The Red Web: the Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. New York: Public Affairs; Georgetown University, Azhar Unwala, Shaheen Ghori, National Defense University. 2015. "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict." *Military Cyber Affairs* 1 (1): 1–13.

requesting the extradition of former SBU leader Oleksandr Yakymenko[29] and it further aligns with reports about SBUs significant penetration by Russian intelligence.[30] Within one year of Euromaidan more than 325 SBU officers had been removed and 25 had been charged with treason and all regional directors had been replaced.[31]
Changes in personnel within government ministries while normal under political transitions occurred across all government ministries and agencies in Ukraine. Systemic underfunding of the defense sector combined with rampant corruption set the post-revolutionary status of the military in a perilous position.[32] In 2014 Ukraine out of a total active military force of 129,950 only 6,000 troops were combat ready and able to counter Russian intentions in Crimea and in Eastern Ukraine.[33] Every organization under the control of Ukraine's National Security and Defense Council was impacted by the change in governance. Many of the former heads of ministries fled the country and ended up in Russia.

The re-establishment of reasonable functional governance within Ukraine in March 2014 began with the realization that 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 result was a power vacuum in Ukraine.[34] This effectively left a large number of mid-tier bureaucrats with an existing bureaucratic culture in place while the temporary government and subsequently the new administration of Petro Poroshenko appointed new leadership to replace the old. As noted by James Q. Wilson, bureaucratic cultures once entrenched can make change extremely difficult and often frame the manner in which institutions address challenges.[35]

While the Ukrainian higher political architectures were new, and the heads of ministries were new, change in addressing issues related to cybersecurity and information security were slow and bogged down in conventional inter-ministry bureaucratic relations. The status quo prevailed at the functional level of government. Furthermore, because of ongoing crises associated with kinetic activities on Crimea and in Eastern Ukraine, little thought was given to unfolding cyber and information warfare activities. Moreover, the new government, in particular MPs within the Verkovna Rada with nationalist orientations failed to fully appreciate the extent of Russian information interference and the impact that their actions might have on the further exacerbation

[29] 2015. "Ukraine Accuses Russia of Breaking CIS Agreements Over Yanukovych Extradition." *Interfax-Ukraine*. January 12. https://en.interfax.com.ua/news/general/243934.html.
[30] Miller, Christopher. 2014. "Ukraine's Top Intelligence Agency Deeply Infiltrated by Russian Spies." *Mashable*. December 30. https://mashable.com/2014/12/30/russian-vs-ukrainian-spies/.
[31] Ibid.
[32] Oliker, Olga, Linn E Davis, Keith Crane, Andrew Radin, Celeste Ward Gventer, Susanne Sondergaard, James T Quinlivan, et al. 2016. "Security Sector Reform in Ukraine." *Rand.org*; Daalder, Ivo, Michele Flournoy, John Herbst, Jan Lodal, Steven Pifer, James Stavridis, Strobe Talbott, and Charles Wald. 2015. "Preserving Ukraine's Independence, Resisting Russian Aggression." Brookings; 2013. "Government Defence Anti-Corruption Index 2013." Transparency International UK.
[33] Brantly, Aaron F, Nerea M Cal, and Devlin P Winkelstein. 2017. "Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW." West Point, NY: U.S. Army Cyber Institute. http://www.dtic.mil/dtic/tr/fulltext/u2/1046052.pdf.
[34] Ash, Timothy, Janet Gunn, John Lough, Orysia Lutsevych, James Nixey, James Sherr, and Kataryna Wolczuk. 2017. "The Struggle for Ukraine." London: The Royal Institute of International Affairs.
[35] Wilson, James Q. 1989. *Bureaucracy: What Government Agencies Do and Why They Do It*. New York: Basic Books.

of the Ukrainian crisis when they proposed eliminating the status afforded to the Russian language.[36] Although 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.

Within weeks of the completion of the successful revolution, Ukraine began to increasingly suffer at the hands of sustained information operations and limited cyber operations. The pernicious nature of Russian propaganda as measured by the Kyiv International Institute of Sociology indicates strong effect 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.[37] The impact of propaganda targeted at the Eastern Oblasts was four times as impactful as the same propaganda directed against Western Oblasts.[38] In discussions with faculty at the National University of Kyiv-Mohyla's StopFake.org project and with various faculty at Taras Shevschenko National University of Kyiv, discussions on the pervasiveness and impact of disinformation and propaganda in Ukraine gave faculty and students the impression of an information siege seeking to systematically undermine the fabric of the Ukrainian state. StopFake.org both in their discussions in 2017 and 2018 as well as materials provided by their organization indicated a sustained effort to challenge fact-based understandings of events at almost every turn.

One of the most egregious examples of the early information war occurred when a Buk missile (surface-to-air missile) was fired from rebel held territories in Eastern Ukraine.[39] The violence of the attack was matched by the voluminous attempts by the Russian Federation to seek to pin the blame for the attack on Ukraine.[40] It took outside investigative organization BellingCat to provide substantial evidence in the form of photographs and videos of the Buk missile system in rebel held territory both before and after the attack (missing a missile) to squarely place blame on the Russian Federation and its proxies.[41] It would take the a Dutch criminal investigation 4 years to complete an investigation and formally hold the Russian Federation accountable.

Although a great deal of emphasis has been placed on the cyber aspects of the conflict the information warfare aspects enabled through cyberspace rose rapidly to prominence and has been extensively examined.[42] In May 2017 President Poroshenko in the face of continued information

---

[36] Kudriavtseva, Natalia. 2016. "Ukraine: What's a Language for?." *Kennan Cable* 15 (March). Washington, D.C.: 1–9.
[37] Ibid.
[38] Ibid.
[39] "MH17: Evidence mounts against Russian-backed separatists; Ukraine interior minister claims Buk missile launcher moved across border to Russia, as accident investigators raise fears about interference at crash site." Telegraph Online, July 18, 2014. Infotrac Newsstand (accessed September 19, 2018). http://link.galegroup.com.ezproxy.lib.vt.edu/apps/doc/A375333208/STND?u=viva_vpi&sid=STND&xid=d797a98c.
[40] Fitzgerald, Chad W, and Aaron F Brantly. 2017. "Subverting Reality: the Role of Propaganda in 21st Century Intelligence." *International Journal of Intelligence and CounterIntelligence* 30 (2): 215–40.
[41] 2017. "The Open Source Investigation Three Years Later." BellingCat. https://www.bellingcat.com/wp-content/uploads/2017/07/mh17-3rd-anniversary-report.pdf.
[42] Georgetown University, Azhar Unwala, Shaheen Ghori, National Defense University. 2015. "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict." *Military Cyber Affairs* 1 (1): 1–13; Jaitner, Margarita, and Peter A Mattsson. 2015. "Russian Information Warfare of 2014." In, 1–14. Tallinn; Snegovaya, Maria. 2015. "Putin's Information Warfare in Ukraine." Washington, D.C.: Institute for the Study of War.

operations by Presidential decree blocked access to a variety of Russian social media, news and other technology sites.[43] The decree on the blockage of various information outlets occurred at the beginning of the interview and meeting schedule in Ukraine. Every individual or organization had nearly the same response: "we are under attack, we must protect the nation." When probed further Ukrainian academics further acknowledged the poor precedent the decree established with regards 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. These nationalistic efforts to foster unity began shortly after the new government took office. Simultaneously, generally positive support, through Facebook groups, civil society organizations, 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 dozens of volunteer battalions engaged in sustained conflict operations with limited supply lines and little to no medical assistance.[44]

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.[45] 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.

The success of the information operations against frontline soldiers and volunteers was the result of a confluence of events in the early days of the conflict including a lack of secure radios or a lack of training on those radios. Many of these same challenges persist to the present and the result is the continued use of mobile devices, in particular inexpensive Android phones by soldiers. Soldiers received messages telling them that they were going to die, that their bodies would "freeze in the snow," that their families wouldn't know they were dead and more. Additionally, soldiers interviewed also indicated that their family members received text messages and SMS/MMS messages purporting to be from them while they were serving on the front lines. These messages told family members the soldier was dead or that they should convince him to come home.[46]

---

[43] 2017. "Ukraine Country Report | Freedom on the Net 2017." Washington, D.C.: Freedom House.
[44] Marten, Kimberly, and Olga Oliker. 2017. "Ukraine's Volunteer Militias May Have Saved the Country, but Now They Threaten It." *War on the Rocks*. September 14. https://warontherocks.com/2017/09/ukraines-volunteer-militias-may-have-saved-the-country-but-now-they-threaten-it/.
[45] Brantly. "Defending the Borderland"
[46] Ibid.

Asked whether the Ukrainian Military was addressing these concerns, senior leaders indicated that the military was not able to address these concerns due to fiscal, technical, and human resource challenges. Most distressing were soldiers' responses to targeted information operations and the continued use of insecure devices with the simple statement "we have to live." Indicating a strong reluctance to relinquish the devices both because they would be unable to communicate on the contact line and because their device however penetrated and used as a vehicle for information operations targeted against them and their fellow soldiers was a desired lifeline to the normalcy of their lives in Ukraine.

To date the overwhelming response of Ukraine to information warfare has emphasized three distinct categories and styles of approach. First, several organizations within Ukraine and others outside of Ukraine have been heavily engaged in processes of identification and correction of information operations through organizations such as StopFake.org and InformNapalm.org and others. These campaigns vary in intensity, impact and breadth. They are not systematic and are poorly resourced but have gained international attention, funding, and are thought to have reasonable impact. Ukrainian and foreign journalists interviewed indicated these platforms offered a means of informed counter information warfare that sought to confront information warfare using facts and logic. InformNapalm, takes the counter information operations a degree further and engages in cyber operations and other activities to actively seek out information both legally and illegally obtained for counter information warfare and endogenous propaganda efforts.

Second, a variety of government initiatives both legislated and by decree have been undertaken in Ukraine to foster both resilience and combat information warfare. In December 2014 the Verkhovna Rada of Ukraine established the Ministry of Information Policy (MIP).[47] 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."[48] The creation of the MIP raised concerns that it might transform into an Orwellian information ministry that controls and regulates free speech.[49] Generally the MIPs was designed to work with journalists, foster national media literacy, emphasize counter information operations in the ATO (Eastern combat zone), 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 OSINT academy that developed digital courses on information verification.[50] The efforts of the MIP have been moderately successful but lacks substantial funding and suffers from potential reputational challenges due to its inherent function.

The Ukrainian government by Presidential decree has not only closed access to various web platforms it has also selectively enforced legal statues 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

[47] Matychak, Tetiana. 2017. "David Against Goliath: How Ukraine Resists the Kremlin's Information Attacks." In *Words and Wars: Ukraine Facing Kremlin Propaganda*, edited by Andriy Kulakov. Kyiv: Internews-Ukraine.
[48] https://mip.gov.ua/files/documents/Concept.docx
[49] Miller, Christopher. 2014. "Ukraine Just Created Its Own Version of Orwell's "Ministry of Truth"." *Mashable*. December 2. https://mashable.com/2014/12/02/ukraine-ministry-of-truth/.
[50] Matychak. "David Against Goliath."

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 three years managed to distribute on a near daily basis maps indicating their perceived status of forces along the ATO 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.[51] 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 policy-makers. All of these organizations form a counter information operations cachophny that was non-exisitent in 2013 and early 2014. While Ukraine is still susceptible to information operations, its resilience has increased markedly.

One area were information operations have evolved substantially since 2014 is in Eastern Ukraine, the creation of Army FM radio funded the Spirt of America Foundation runs a 24 a day radio broadcast. In meetings and discussions with Radio FM and funders they were clear to indicate that they promoted the unified vision of Ukraine but were intent on adhering to fact-based reporting along the ATO. Army FMs towards were primarily directed towards Ukrainian personnel along the ATO and those individuals immediately across the contact line. They often take up issues in Russian media and provide a Ukrainian perspective.

Although many of the initiatives undertaken by Ukraine and partners have improved, the status of information balance between the two parties 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.[52] 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 is 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

[51] http://ukraineworld.org/infowars/

[52] Karatnycky, Adrian. 2018. "The Rise and Fall of Mikheil Saakashvili." *Politico*. February 12. https://www.politico.eu/article/the-rise-and-fall-of-mikheil-saakashvili/.

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 Cybersecurity Challenges – A Centralized Approach

Whereas the information warfare situation in Ukraine has been addressed by both a decentralized non-governmental and centralized governmental approaches, the cyber conflict in Ukraine has primarily been confined to state bureaucracies. As noted by Nadiya Kostyuk, Ukraine has historically been a hotbed of global cybercrime.[53] This is despite Ukraine's affirmation of the Budapest Convention on Cybercrime and laws on its books dealing with cybercrime. Ukraine is in an interesting position visa-a-vis cyber capacity. Ukraine produces excellent students with STEM (science, technology, engineering, and mathematics) backgrounds, suffers immensely from economic challenges and a poor political and a burdensome business regulatory environment, and a perception, rooted in social norms that cybercrime directed against non-Ukrainians constitutes hooliganism rather than a "serious" crime.[54] Throughout the 1990s and 2000s Ukraine was designated a priority foreign country for its substantial violations of intellectual property rights (IPR).[55] So bad was Ukraine's adherence to IPR, 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.[56]

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 ageing soviet infrastructure, penetrated intelligence services, firms owned in part by Russian interests and a variety of other market and criminal concerns left Ukraine extremely exposed to potential cyber exploitations. Cyber exploitations came in droves and continue to persist 4 years after initial hostilities. Marie Baezner and Patrice Robin from the Center for Security Studies (CSS) at ETH Zurich combined a list in 2017 outlining many of the major cyber incidents that occurred over the course of the conflict through December 2016.[57] Their list indicates a disproportionate number of government targets, 29 out of 64 incidents, and a disproportionate number of actors attacking Ukrainian institutions or individuals

[53] Kostyuk, Nadiya. 2015. "Ukraine: a Cyber Safe Haven?." In *Cyber War in Perspective: Russian Aggression Against Ukraine*. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.
[54] Ibid; These factors were also identified repeatedly in discussions at Kyiv Polytechnic National University and with members of the defense industrial base.
[55] 2001. "USTR - Ukraine Designated as Priority Foreign Country Under Special 301." *Ustr.Gov*. March 13. https://ustr.gov/archive/Document_Library/Press_Releases/2001/March/Ukraine_Designated_as_Priority_Foreign_Country_Under_Special_301.html.
[56] 2005. "Chairman's News | Newsroom | the United States Senate Committee on Finance." *Finance.Senate.Gov*. November 18. https://www.finance.senate.gov/chairmans-news/grassley-praises-senate-passage-of-jackson-vanik-repeal-for-ukraine.
[57] Baezner, Marie, and Patrice Robin. 2017. "CSS CYBER DEFENSE PROJECT Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict." Zurich: Center for Security Studies, ETH Zurich.

55 out of 64 incidents.[58] The volume and severity of attacks corresponds to discussions held with the NSDC principles responsible for cyber, who indicated systemic attacks against Ukrainian government institutions intended to undermine confidence in the Ukrainian state. The numbers indicated by the CSS research team are non-exhaustive but provide a well-sourced view of the conflict that aligns with the sentiments of Ukrainian officials.

Over the period of March 2014 – June 2018, Ukraine has been the site of some of the most significant cyber-attacks ever perpetrated. As noted by Wired reported Andy Greenberg, Ukraine became the equivalent of a test lab for Russian cyber capabilities.[59] Figure 2 below lists some of the targets of cyber-attacks over time. The emphasis is not on each individual attack, but the process of skill development and capability to attack the Ukrainian state.

Figure 2: Cyber Targets in Ukraine 2014-2018

Target	Year(s)
Opposition Websites	2013-2014
Opposition Mobile Devices	2013-2014
Ukrainian Government Websites	2014, 2015, 2016, 2017
U.S. Diplomatic Communications	2014
Ukrainian Central Election Commission	2014
Ukrainian News Websites	2014, 2015
Ukrainian Banks	2014, 2015, 2016
Ukrainian Soldiers' Phones	2014
Ukrainian Military Email Communications	2014
U.S. Military Contractors in Ukraine	2015
Ukrainian Law Enforcement	2015
Ukrainian Power Grid Attack	2015, 2016
Ukrainian Ministry of Defense	2016
Ukrainian Railway Transport Systems	2016, 2017
Ukrainian Air Transport	2017
Chernobyl Radiation Monitoring System	2017
Ukrainian Accounting Software	2017
Ukrainian Postal Services	2017

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, reduced or halted services. Yet as can be seen the attacks are continuous and escalating in both breadth and severity. To date there is no direct correlation of a cyber-attack in Ukraine resulting in physical death, however, the trajectory of attacks indicates both the evolving extent and organizational shortfalls of Ukraine in cyberspace. 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.[60]

[58] Ibid.
[59] Greenberg, Andy. 2017. "How an Entire Nation Became Russia's Test Lab for Cyberwar." *Wired.com*. June 17. https://www.wired.com/story/russian-hackers-attack-ukraine/.
[60] ICS-CERT, NCCIC. 2016. "IR-ALERT-H-16-043-01BP Cyber-Attack Against Ukrainian Critical Infrastructure," April, 1–17; Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."

Nadiya Kostyuk identified the organizational structure of Ukrainian cyber defense in 2015 as forming within the National Security and Defense Council of Ukraine and encompassing of 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).[61] As of 2015 the coordinating entities of the NSDC related to cyber were managed by a single individual who reported to the Chairman. Despite having an organizational flow chart, as late summer 2017 the capabilities contained within the organizations listed as encompassing of cybersecurity in Ukraine were severely understaffed, suffered from personnel turnover, or simply lacked funding to undertake their stated mission.

In 2015 Ukraine released its first national security strategy. The document included an acknowledgement that Ukraine's cyber infrastructure has been attacked and that the establishment of a formal cybersecurity system emphasizing countering cyberterrorism, protection of critical infrastructures, in particular the military, energy, transportation, and banking spheres was necessary. The document also outlined and proposed that the state would work with NATO and EU members to establish best practices within Ukraine.[62] 10 months after releasing its first national security strategy, President Poroshenko by presidential decree approved on March 15, 2016 the first Cyber Security Strategy of Ukraine.[63] Slightly more than 2 years after the ousting of the Yanukovych government and following more than 50 severe cyber-attacks including those perpetrated against Ukrainian electric infrastructure, Ukraine had a working cyber strategy.

Although a 2-year delay between change of administration and the establishment of a strategy might seem to be a long time the reality is this was a monumental shift in the bureaucratic and functional approaches to national cybersecurity in Ukraine. The reorganization codified through presidential decree the organizational structure of cyber defense under the NSDC. Documents provided by the National Cybersecurity Coordination Center, beneath the NSDC illustrated in Figure 3 indicates the new organizational approach to cyber in Ukraine. While some of the organizations involved remain the same as those indicated in 2015, there are marked shifts through the inclusion of the National Police (a newly established organization in July 2015), the National Bank, and the deliberate inclusion of external partners. Notably the removal of the Ministry of Internal Affairs as a higher-level organizational partner is still represented via its sub organization the National Police of Ukraine.

Wired.com. August 22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; Zetter, Kim. 2016. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid | WIRED." *Wired.com*. March 3. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[61] Kostyuk. "Cyber Safe Haven?"

[62] 2015. *National Security Strategy of Ukraine (DRAFT)*. *Niss.Gov.Ua*. Kyiv.

[63] 2016. *Cybersecurity Strategy of Ukraine*. Kyiv: Office of the President of Ukraine.

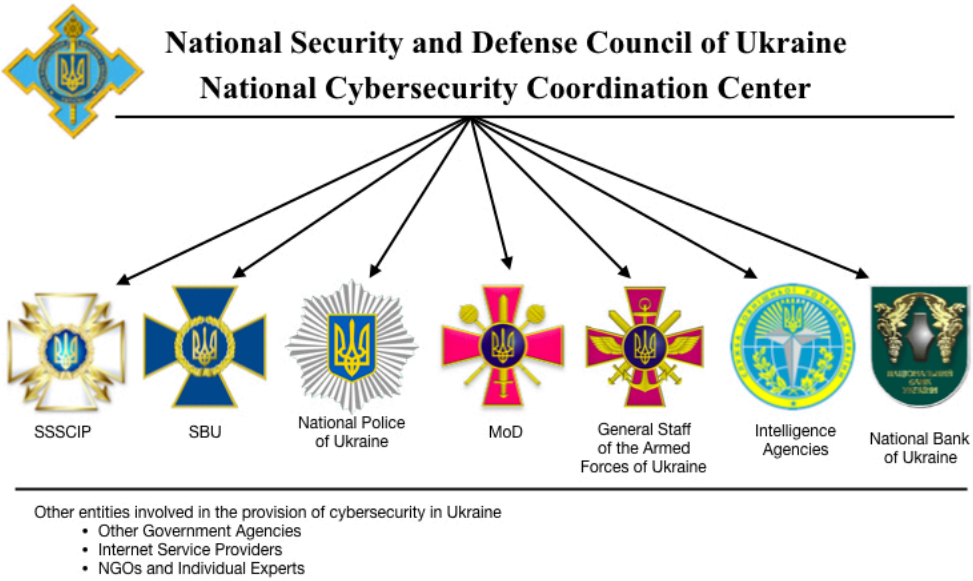

Figure 3: Organization of National Cybersecurity in Ukraine

Procedurally as of 2017 the NSDC Cybersecurity Coordination Center in discussions and in documentation indicated that the implementation and direction of cyber activities in 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. The procedural status of Ukrainian cybersecurity has been further codified in a newly adopted law on national cybersecurity (October 2017). In terms of strategy development, organizational conceptualization, and legal justification and law development Ukraine has moved very quickly. Despite having a variety of information, media, morality and propaganda laws on the books, and despite having a registered CERT, its bureaucracy in 2014 was ill-equipped both organizationally and functionally to deal with the challenges it faced.

Although as of 2017 the organizational and procedural structure of Ukrainian cyber defenses is making substantial strides there remain specific bureaucratic and economic challenges that limit the impact of the organizational change. 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,[64] conversations with principles and subordinates indicated extreme pay disparities between individuals in the public sector and those in the private sector. The disparity indicated by one individual interviewed who left the a national CERT and transitioned to a private defense industrial base CERT resulted in a change in the individual's salary by a factor of 10. The living wage of individuals involved in

[64] Wenger, Jennie W., Caolionn O'Connell, and Maria C. Lytell, Retaining the Army's Cyber Expertise. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1978.html.

government service was identified by all organizations within the NSDC as a significant matter of concern and was also identified in a 2016 RAND report on Ukrainian security sector reform.[65]

Ukraine has and continues to receive international support for a variety of training initiatives. The United States, NATO and various EU countries, the OSCE and others.[66] Funding has provided material resources for the establishment of training centers, equipment for defensive cyber operations, training for police and CERTS and a variety of affiliated projects. More than $1.7 million dollars was committed to Ukraine for cyber defenses by NATO countries.[67] The United States has sent national guard Units to Ukraine to engage in cybersecurity training missions.[68] Yet, despite repeated training, of military and civilian elements of Ukraine's cyber defense infrastructure the skills acquired increase the market prospects of the individuals trained and reduce their willingness to remain in government service. The two exceptions to perpetual staffing challenges identified in interviews and subsequently supported by secondary sources are the National Cyber Police of Ukraine and the Security Services.[69] 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 many of the necessary financial resources required for the development and maintenance of its organizational aspirations for cyber defense, a more serious problem of bureaucratic cultures undermines the ability of Ukraine to systematically establish balanced cyber defenses. In conversations with the MoD, at the NSDC, at the Foreign ministry and at other meetings with individuals or organizations affiliated with the cybersecurity in Ukraine, all indications both in public and private conversations highlighted the disproportionate control of cyber defense within the SBU. News organizations and commentary out of think tanks concur with the assessment that the SBU has, in the wake of the revolution re-established itself and accumulated substantial power with the Ukrainian state.[70]

---

[65] Oliker, Olga, Linn E Davis, Keith Crane, Andrew Radin, Celeste Ward Gventer, Susanne Sondergaard, James T Quinlivan, et al. 2016. "Security Sector Reform in Ukraine." *Rand.org*.

[66] Interfax-Ukraine. 2017. "Ukrainian Cyber Police Receive Special Equipment From OSCE - Jul. 19, 2017." *Kyiv Post*. July 19. https://www.kyivpost.com/ukraine-politics/ukrainian-cyber-police-receive-special-equipment-osce.html; Seals, Tara. 2017. "US Army Funds Cyber-Center for Ukraine Military." *Infosecurity Magazine*. February 2. https://www.infosecurity-magazine.com:443/news/us-army-funds-cybercenter-for/.

[67] 2016. "Ukraine Cyber Defence." *Nato.Int*. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160712_1606-trust-fund-ukr-cyberdef.pdf.

[68] 2018. "EUCOM State Partnership Program." *Eucom.Mil*. Accessed September 21. http://www.eucom.mil/mission/partnership-programs/eucom-state-partnership-program.

[69] Sviatenko, Tetiana. 2018. "Cyber Police: What Are Ukrainian Virtual Cops Doing?." *112.UA*. February 5. https://112.international/article/cyber-police-what-are-ukrainian-virtual-cops-doing-25336.html.

[70] Grytsenko, Oksana, and Oleg Sukhov. 2017. "SBU Out of Control? Secretive Law Enforcement Agency Accused of Abusing War-Time Powers - Sep. 29, 2017." *Kyiv Post*. September 29. https://www.kyivpost.com/ukraine-politics/sbu-control-secretive-law-enforcement-agency-accused-abusing-war-time-powers.html; Halyshka, Olena, and Anastasia Krasnosilska. 2018. "Ukraine's Next Reform Challenge May Be the Toughest One Yet." *Atlantic Council*. June 12. http://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-s-next-reform-challenge-may-be-the-toughest-one-yet.

Some interviewees indicated that funds originally directed by international donors towards other organizations within the family of cyber organizations under the NSDC were confiscated by the SBU and reallocated, thus leaving their organizations unable to address training or resource demands. When confronted on these issues during interviews, the leadership of the SBU provided two competing explanations. First, that the SBU based on the nature of the conflict in Ukraine had a constitutionally privileged role in responding to "terrorist" activities. Second, SBU officials indicated that concerns about the consolidation of power and therefore resources in the SBU was nothing more than bureaucratic infighting by organizations that felt they had not received their fair share and wanted more.

There is little data to substantiate the arguments either way and the funding currently received in Ukraine and distributed to various entities does appear to be having a moderate effect. Ukraine is presently participating in international training activities such as NATO's Cyber Defence Center of Excellence exercise Locked Shields.[71] Each new attack is often followed by a period of increased financial and technical support from European, US and NATO allies.[72] Yet, despite increasing external support, the status quo of cybersecurity in Ukraine remains inadequate.[73] Efforts to appropriately distribute resources do appear to be achieving some success, particularly in areas of critical infrastructure.[74]

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 cybersecurity, it has reorganized and established cyber as a core component of the NSDC. It has written and approved a national cybersecurity strategy and it recently passed national cybersecurity 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.

Ukrainian Cyber and Information Security in the Present and Future

It would be inaccurate to say that the bureaucratic cultures of Ukraine have fundamentally changed. They 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 4 years, with external help from foreign states, international organizations and non-profit assistance has been substantial. It is hard to over-state the challenges Ukraine faced in 2014 and

---

[71] Zilberman, Boris, and Trevor Logan. 2018. "Increasing U.S.-Ukraine Cyber Cooperation Is a Step in the Right Direction | Foundation for Defense of Democracies." *Defenddemocracy.org*. May 15. http://www.defenddemocracy.org/media-hit/boris-zilberman-increasing-us-ukraine-cyber-cooperation-is-a-step-in-the-right-direction/.

[72] Paganini, Pierluigi. 2017. "Following NotPetya NATO Increases Support for Ukraine's Cyber Defenses." *Security Affairs*. July 12. https://securityaffairs.co/wordpress/60941/cyber-warfare-2/nato-support-ukraine-cybersecurity.html; Lyngaas, Sean. 2018. "State Department to Double Cyber Defense Aid to Ukraine - CyberScoop." *Cyberscoop*. May 3. https://www.cyberscoop.com/state-department-ukraine-cyber-aid/.

[73] Williams, Matthias. 2017. "Ukraine Finally Battens Down Its Leaky Cyber Hatches After Attacks." *Reuters*. August 1. https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN1AH35A.

[74] 2018. "Ukraine Power Distributor Plans Cyber Defense System for $20 Million." *Reuters*. February 6. https://www.reuters.com/article/us-ukraine-cyber-ukrenergo/ukraine-power-distributor-plans-cyber-defense-system-for-20-million-idUSKBN1FQ1TD.

how far it has come. Its approaches to national information security and national cybersecurity have taken markedly different paths and have achieved fundamentally different outcomes. Ukraine still suffers from information warfare attacks and from cybersecurity attacks, but it is hard not to assess that Ukraine is more resilient to Information warfare now than it was in 2014. By contrast it is difficult to make the same assessment of the cybersecurity environment of Ukraine.

Information security and cybersecurity require different infrastructural and organizational structures and capabilities. Both however impact governmental organizations and society at large. 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 cybersecurity is not. As concepts of national pride and identity, laws on the prevention of disinformation and propaganda pervade the population of Ukraine is likely to increase rather than decrease its resilience to outside manipulations.

The development of cybersecurity structures in Ukraine, by contrast, has been highly centralized. The organizations that became responsible for cybersecurity 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 cybersecurity concerns, yet each organization, by necessity had many other priorities that often superseded cybersecurity.

Few countries have been so strenuously tested 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 at the highest levels and often stifle the innovation and aspirations of mid-level bureaucrats. 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 sustain 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 cybersecurity. Finally, if Ukraine is unable to foster coordination and cooperation amongst the various NSDC entities then duplication of effort, interagency animosities and inadequate cybersecurity outcomes are likely.