16
IN THE LINE OF RUSSIAN UKRAINE, HYBRID WARFARE, AND CYBERSECURITY DEFENSE AGGRESSION

Ukraine, hybrid warfare, and cybersecurity defense

Olya Zaporozhets and Oleksiy Syvak

Introduction and background

Once a Soviet Union republic, Ukraine gained its independence after the Soviet Union collapsed in 1991. At that time 84 per cent of Ukrainians took a referendum vote in support of the Act of Declaration of Independence of Ukraine. This is an important fact to note for the future discussion of a hybrid war between Russia and Ukraine. The referendum of 1991 included Ukrainian citizens in Crimea and eastern Ukrainian territories whose decision to be a part of independent Ukraine was questioned by Russian President Putin in 2014. Putin justified his invasion of the Ukrainian territories by claiming that its purpose was to “protect Russian speaking population of Ukraine.” That claim, like every other in informational wars, was only partially true as many villagers in eastern Ukraine spoke Ukrainian or a mix of the two languages and the majority of them supported the decision for Ukrainian independence with the National Referendum of 1991 and at the time of the Russian invasion in 2014.

The 1991 Declaration of Independence of Ukraine and the referendum provided a new historic beginning where this Eastern European nation of about 52 million people at the time started its path to democracy, breaking bounds with socialism and building democratic institutions, a free economic market, and new international relations. The initial years of Ukrainian independence were marked by a drastic economic crisis, formation of oligarchic elites, and the growth of corruption. Strategically located between Russia and the NATO countries of Slovakia, Hungary, Poland, and Romania, Ukraine was ambivalent in its foreign policy towards Europe, the US, and NATO, on the one hand, and towards Russia and the Customs Union that consisted of some former Soviet republics, on the other. Perhaps a bit naively, the Ukrainian government sought to cement its friendships with the West and
East by signing the Budapest Memorandum (1994), where it surrendered the world’s third largest nuclear arsenal in exchange for guarantees of its territorial integrity and security from Russia, Great Britain, and the United States, initial signers of the memorandum, and later co-signed by France and China. For two decades after proclaiming its independence, many Ukrainians seemed to believe that there were no valid external threats to Ukrainian national security: the Russians were family and the West was friendly and civil.

However, the situation rapidly shifted as the Ukrainian government negotiated the European Association and Free Trade Agreement with the EU in 2014. Russia saw the threat of Ukraine joining the European community as it could mean NATO borders extending to the Russian backyard and Ukraine leaving the Russian sphere of influence. As Ukrainian President Yanukovich found himself caught in this East and West dilemma and refused to sign the European Association Agreement, the Ukrainian people started peaceful protests that lasted for three winter months and progressed to bloody street fights where over 100 protesters were shot. This protest was called the Revolution of Dignity, which only became possible with the utilization of real-time broadcasting, good communication between the protesters, and the ability to evaluate sources of information in initially government-controlled and Russia-influenced media communications. That experience was remarkable as we consider strategies for building national informational defense systems and bringing awareness about cybersecurity among the general public.

The Revolution of Dignity led to Yanukovich leaving office and fleeing to Russia. After that the Ukrainian Parliament (Verhovna Rada of Ukraine) appointed a transitional government and reelections. At this time of vulnerable transition, Russian President Putin invaded the Ukrainian Crimean Peninsula with a further illegal referendum and annexation that was not recognized by the international community. This was the first incident when Russia annexed occupied territories, as in the instances with Abkhazia, South Ossetia, Transnistria, and Nagorno-Karabakh, where Russia first would start with military aggression, then form the puppet governments of so-called people republics, but did not proceed to the official annexation of those territories. Apparently, the need for restoration of the Russian greatness in Russian society was so significant that it certainly outweighed the risks of international community reaction to this situation. Western leaders and international organizations were unable to enforce international law during previous Russian military occupational campaigns, so Putin, perhaps, decided to raise his electoral ratings with this Tsar conqueror invasion. In response, Ukraine proclaimed its territory as being occupied and appealed to the signers of the Budapest Memorandum to protect the integrity of its territory as one of the country-signers conducted the attack. That appeal was to no avail.

After the Crimean Peninsula occupation, Russia moved to gain control over Ukrainian eastern and southern territories, first by means of Russian inspired protests led by Russian special forces officers that soon turned into open military aggression by the Russian army with the use of hardware military equipment. It became known as the Russian Spring operation. The advancement of Russian military forces was stopped by the combination of revolution-inspired Ukrainian volunteer military groups and Ukrainian active duty military forces. NATO and Budapest Memorandum signers were unable to render any military support to Ukraine at that time. Russia gained control of 8 per cent of the Ukrainian territory that consisted of one third of two Ukrainian regions (oblasts) – Donetsk and Luhansk oblasts. This territory and Ukraine in general further became the field of a new hybrid war and a lab for Russian cyberattack training, which presented Ukrainians with unlimited opportunities to develop, update, and perfect informational defense and cybersecurity systems.
Hybrid war

To help illustrate Ukrainian–Russian hybrid warfare, there was one particular incident that deeply shocked and awakened the international community. It was the shooting down of the Malaysian commercial flight with the Russian Buk surface-to-air missile, a weapon of massive destruction, at an altitude of 33,000 feet in July of 2014. All 298 flight passengers and crew members were killed, out of which 80 passengers were children. Of course, the operation of surface-to-air missile equipment required several years of specialized military college training and, apparently, could not be done by anyone but Russian soldiers. The question remains, however, about the purpose of this attack in the context of Ukrainian–Russian hybrid war.

According to the head of the Security Service of Ukraine (SSU), Valentin Nalivaychenko (in office 2014–2015), the Buk crossed the Russian–Ukrainian border the night before the incident, and Russian soldiers simply confused two villages with the same name, Pervomayskiy. As a matter of fact, Donetsk area had as many as seven villages and towns with that same name. At the time of the incident there were two planes in the airspace flying at similar heights, one was Malaysian MH 17 and another one was Russian, Aeroflot flight SU2074. Nalivaychenko presented evidence that the Russian plane was the real target, not the Malaysian one, as its shooting down was supposed to create for Russians the “casus beli,” the situation that would justify open Russian invasion of the Ukrainian territory (Espreso.TV, 2016).

This incident illustrates the essence of the informational war, how reality and facts can be distorted or confused to support conventional military operations. This also gives an insight into the kinds of challenges that Ukrainian military, Security Service, and Ukrainian people in general have to face daily in the area of informational defense in addition to typical challenges that are faced by any computer user, business, or government organization in every country of the world. According to the Head of Informational Security and Cyberdefense Council of Ukraine, Ellina Shnurko-Tabakova, the cybersecurity challenges of Ukraine are similar to other countries; Ukraine has “just as much [cyber] stealing as anywhere else in the world … however, the rate of cyberaggression in Ukraine with no commercial interest is the highest in the world,” she adds (personal communication, July 27, 2019). Shnurko-Tabakova further explained that the cyberattacks on business and government organizations are often done by Russian special forces as they are conducted in support of and in tandem with conventional Russian military actions. For example, the naval operations website was under cyberattack at the time of the Russians attacking and seizing Ukrainian military ships in Kerch Strait in November 2018. This cyberattack created barriers for the Ukrainian naval operations office to communicate about this incident for approximately five hours while the international community was struggling to learn the details about this situation and understand the facts in the news stream (Ellina Shnurko-Tabakova, personal communication, July 27, 2019).

The intent of Russian cyber- and informational attacks has also a purpose of psychological influence, such as discreditation of government or military leadership, especially during the time of critical military operations. As noted in Ukrainian scientific cyberliterature, informational attacks have a purpose of bringing chaos, challenging or breaking organizational structures, and causing emotional distress or turmoil to the point of self-destruction (Vorobyova, 2010). One example of informational attack in a hybrid war was evidenced during the Battle of Debaltseve. The Ukrainian military was surrounded by Russians in Debaltseve in Eastern Ukraine in January 2015, which resulted in 267 Ukrainian military deaths and over 100 military personnel taken captive. At the time of this operation, Russians spread messages
through the news and social networks that Ukrainian generals were incompetent and unable to foresee a surrounding that apparently was obvious to all internet users. This, of course, presented a distorted picture of real facts which became exceptionally dangerous as sharing true facts by Ukrainian generals in that situation could lead to casualties in real time military operation. Again, this incident illustrated how the informational attack was synchronized with the military operation to magnify the offense impact. Such complex informational and cyberdefense situations require multilevel preparation and response, which we will discuss next.

Challenges of cybersecurity defense in the hybrid war

The first challenge that Ukraine faced in the Russian hybrid war was the inconsistency of Soviet and NATO cybersecurity standards. It is important to note that Ukraine inherited Soviet informational defense systems that, at the time of the Russian invasion, were dated and ineffective as they were based on the 1990s standards that were created before the internet became available to users, explains Ellina Shnurko-Tabakova (personal communication, July 27, 2019). The original Ukrainian Complex Informational Defense System is geared towards regulating physical requirements for data storage, coding, and location, while alternative EU and NATO security standards are concentrated on risk management, preparedness, and prevention that is described by the Informational Security Management System.

The hybrid war with Russia prompted the Ukrainian government to pass several informational defense laws and Presidential Mandates that set up a road map for reformation of the Ukrainian informational defense systems to adequately meet contemporary cybersecurity challenges. One such key Ukrainian document was the Strategic Defense Bulletin of Ukraine (2016) that focused on alignment of Ukrainian defense standards with the defense standards of NATO and the EU with the deadline of 2020 (see, Указ Президента Украины Про рішення Ради національної безпеки та оборони України від 20 травня 2016 року “Про Стратегічний оборонний бюлетень України” [The Mandate of the President of Ukraine about the Decision of the National Security and Defense Counsel of Ukraine “About Strategic Defense Bulletin”], 2016). The Ukrainian government also moved on identification of the cybersecurity problems and governmental structures responsible for cybersecurity defense and protection of people, outlining strategic goals and functions in the cybersecurity law “About Basic Principles of Cyber Security” of Ukraine, passed in 2017 (see Закон України Про основні засади забезпечення кібербезпеки України [About Basic Principles of Cyber Security of Ukraine], 2017).

While this law was criticized by the Ukrainian cybersecurity professional community for the lack of specificity and inefficiency, it allowed Ukrainian governmental and military agencies to start the process of incorporating western cybersecurity standards into their frequently outdated organizational systems and set up the course for their reformation. It also allowed business organizations to switch their focus from the obligation to fulfill certain static system defense requirements to more attuned and updated risk management systems. In addition, the Ukrainian president passed the decree where Ukrainian providers were not allowed to offer internet services that were operated on Russian servers and resources (e.g., mail.ru, yandex.ru etc.) (see, Указ Президента України Про рішення Ради національної безпеки та оборони України від 28 квітня 2017 року “Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)” [The Mandate of the President of Ukraine about the Decision of the National Security and Defense Counsel of Ukraine “About Application of Special Personal Economic and other Restrictive Measures
(Sanctions), 2017). This mandate had an intent to limit the leaks of data and sensitive personal information to the Russian special cyber forces.

With all of this being said, it is also important to note the role of the volunteer civilians and organizations in reformation and cyber protection. Because the Revolution of Dignity had a strong democratic movement, the defense from Russian aggression that followed also inherited unprecedented support from the civil volunteer movement. Small and large civil volunteer groups and individuals actively responded to the needs of the military by the direct provision of equipment purchased from personal and donor funds, often imported from abroad. Perhaps, surprisingly for many, the update of military communication systems at that time also happened in a similar manner, where Ukrainian volunteers decided that purchasing IP telephony communication systems, which matched western standards, was more economical and presented a better communication solution for military needs than Ukrainian standard alternatives. Therefore, very early on in the hybrid war with Russia, Ukrainian military units were functioning with contemporary IP telephony communication equipment that was not in compliance with Ukrainian legislation and military regulations at that time. That, perhaps, gives a surprising insight, that like any other democratic change, cybersecurity informational defense preparedness in general could be initiated by the people and later legalized by the government.

This opens another important topic of discussion in cybersecurity and defense, an informational education of lay people that needs to start in elementary school. Ellina Shnurko-Tabakova shared that Ukrainian secondary schools and colleges started offering the Introduction to Cybersecurity class as the Ukrainian government recognized the need for each Ukrainian student to be able to critically evaluate the source of information, check the validity of facts, and protect devices from viruses (personal communication, July 27, 2019).

At the end of the day, strong cybersecurity and informational defense are not defined by the response to the attack, but rather by the preparedness to prevent those attacks before they happen. “You should always overestimate your enemy and be ready,” Shnurko-Tabakova adds (personal communication, July 27, 2019).

**Conclusion**

Ukraine’s experience is unique as it has a direct hybrid war experience with Russia and was able to successfully mitigate the effects of purposeful Russian cyberattacks over the progression of the hybrid war, frequently unnoticed by the general Ukrainian public. Ukraine inherited Soviet systems of informational defense that were outdated at the beginning of the Russian–Ukrainian hybrid war. In such a situation Ukraine was able to make several impressive strides on multiple levels: legislative, people awareness, technological modernization of organizational equipment systems, and education. There is a lesson that Ukraine has to offer to the international community: not to be naïve about the enemy and be ready for the attack before it starts.

**Suggested reading**


References


Указ Президента України Про рішення Ради національної безпеки та оборони України “Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)” [“The Mandate of the President of Ukraine about the Decision of the National Security and Defense Counsel of Ukraine ‘About Application of Special Personal Economic and other Restrictive Measures (Sanctions)’”], No. 133/2017 (2017, April 28). www.president.gov.ua/documents/1332017-21850