Cyber Operations at Maidan: A First-Hand Account

by
Glib Pakharenko

Chapter 7 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

In Chapter 7, ISACA Kyiv researcher Glib Pakharenko has written a first-hand account of cyber attacks during the revolution in Ukraine. At the EuroMaidan street demonstrations, there were physical and logical attacks against opposition servers, smartphones, websites, and Internet accounts; the most serious incidents coincided with the lethal shooting of protestors. In Crimea, attacks ranged from severing network cables to commandeering satellites to wholesale changes in Wikipedia. In eastern Ukraine, cyber espionage such as the use of location data from mobile phones and Wi-Fi networks has aided in targeting Ukrainian army units; the region has also been isolated from the rest of Ukraine by Internet censorship and regular forensics checks on citizens' computers and mobile devices. Pakharenko ends this chapter by providing the Ukrainian Government with a significant 'to do' list of best practices in network security.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication. Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation. Please contact publications@ccdcoe.org with any further queries.

Cyber Operations at Maidan: A First-Hand Account

Glib Pakharenko
ISACA Kyiv

1 Introduction: Cyber Conflict in Ukraine

I would like to tell the story of what I experienced in Ukraine from the autumn of 2013 until the end of 2014. In this chapter, I will describe the nature and impact of numerous cyber attacks that took place during our revolution and the subsequent conflict between Ukraine and Russia.

As background, it is important to understand the strategic value of Ukraine to Russia. Ukraine is the largest country in Europe, with over 42 million citizens and 27 administrative divisions. In the past, its rich farmland and industrial base have been coveted by Russia, Turkey, Poland, and even by Nazi Germany. Ukraine has also made significant contributions in politics; the Ukrainian Cossacks created the first constitution in contemporary European history. Following the horrors of World War II, the country continued to suffer under Soviet rule until it regained its independence in 1991. Despite that, Russia has never really let go of Ukraine.

Ukraine has had internet connectivity since 1990. As everywhere else in the world, it has also had its share of cyber attacks. The majority of these have come in the form of Distributed Denial-of-Service (DDoS) incidents against politically or economically targeted websites. During election seasons, for example, hackers have frequently gone after the websites of political parties. In terms of cyber crime, Ukraine has long been home to carding, mobile operator fraud, spam factories, cyberlockers, pirated software, unauthorized bank transfers, and various attacks on rival businesses.

Responsibility for the enforcement of internet security in Ukraine belongs to the Ministry of Internal Affairs (MVS) and the Security Service of Ukraine (SBU).[1] Cyber security regulations are overseen by the State Service of Special Communication and Information Protection (SSSCIP),[2] but the ultimate responsibility for cyber crimes has never made explicit, and in this regard there has been competition between the MVS and SBU. Ukraine's Computer Emergency Response Team was created in 2007.

National cyber security legislation is still in its nascent stages. Many of our current laws date from the Soviet era, and need to be updated for the information age. The national critical infrastructure domain is still largely unregulated. Definitions related to 'cyber security' and 'information security' are unclear, as is the distinction between them.

Historically, the Ukrainian police have investigated straightforward cases related to illegal content, online gambling, and pornography. Their number of qualified personnel trained in cyber security was low, with little competency in computer or network forensics. Therefore, their most common tactic was simply to confiscate all IT equipment.

Given these circumstances, Ukraine is currently ill-prepared to combat advanced, nation-state level cyber attacks. In the future, its specialists would like to see the arrival of more non-governmental organisation (NGO) support from the European Union and United States, with a view to implementing modern best practices and internationally recognised standards.

2 The Impact of Euromaidan

The 'Revolution of Dignity' in Ukraine began in late 2013 when citizens took to the streets to vent their fury at the decision of then-President Viktor Yanukovych not to sign an agreement of political association with the European Union (EU). This political movement became known as 'Euromaidan' – the Ukrainian word *Maidan* means 'square' in English, and refers to the main square in the capital city, Kyiv.

On November 30, mobile phone communications were systematically shut down through mobile operators, and armed police units physically attacked the protesters. However, the population was undeterred, and by December 2, more than 500,000 people crowded into *Maidan*. The sitting government made several more attempts to clear the city, using gas grenades and plastic bullets, and the author personally suffered a long-term injury from exposure to tear gas. The crackdown eventually led to the use of lethal force,[3] likely killing well over 100 protestors.[4]

1 The SBU is a former constituent part to the Soviet KGB, and is still coming to terms with its legacy ideology and post-Soviet corruption.

2 The SSSCIP was a former constituent part of SBU and has since had a conflicting relationship with its former parent over its role in the information security arena.

3 The author believes that Russian Security Services took part in these killings.

4 'List of people killed during Euromaidan', Wikipedia, https://en.wikipedia.org/wiki/List_of_people_killed_during_Euromaidan.

The cyber attacks began on 2 December 2013 when it was clear that protesters were not going to leave *Maidan*. Opposition websites were targeted by DDoS attacks, the majority of which came from commercial botnets employing BlackEnergy and Dirt Jumper malware. Police confiscated mobile phones to acquire the protestors' web, email, social media, and financial activities. In one case, pornographic images were uploaded to a protestor's social media account, and were later used to prosecute him. Police seized computers from the opposition party's premises, and according to one city official, the lighting in city hall (which had been a base of opposition activity) was switched off remotely, via the internet.

The cyber attacks began on 2 December 2013 when it was clear that protesters were not going to leave Maidan.

Opposition activists also conducted cyber attacks against the Ukrainian Government, using tools such as the Low Orbit Ion Cannon (LOIC) to launch DDoS attacks on the President's website. When one group of protestors entered the Ministry of Energy, the organisation sounded a 'red alert' at Ukrainian nuclear facilities, due to the fact that the national electricity grid is remotely controlled via the internet from headquarters.

During this period of intense cyber attacks in Ukraine, cyber criminal organisations proactively reduced their use of the Ukrainian Internet Protocol (IP) space, rerouting their malware communications through Internet Service Providers (ISP) in Belarus and Cyprus, which meant that, for the first time in years, Ukraine was not listed among the leading national purveyors of cyber crime.[5]

The largest and most sophisticated attacks coincided with the lethal shooting of protestors in *Maidan* (February 18-20, 2014). The mobile phones of opposition parliament members were flooded with SMS messaging and telephone calls in an effort to prevent them from communicating and coordinating defences. One precision attack (which targeted the protesters on only one street in Kyiv) entailed spamming the IMSI catcher device on mobile phones with fake SMS messages, threatening the recipient with prosecution for participation in the protest.[6]

In western Ukraine, the Government turned off the main opposition TV channel, and when protesters decided to enter police departments, those facilities were disconnected from the Public Switched Telephone Network (PSTN) and internet.

Despite all of these police actions, the now-radicalised protesters were unbowed, and continued their revolutionary campaign. Therefore, on February 22, 2014, Ukrainian President Yanukovich fled to Russia, and a new and reformist government was established in Kyiv.

5 HostExploit analysis, http://hostexploit.com/.
6 This tactic has also been used by Russian military units in eastern Ukraine.

3 Crimea and Donbass

By the end of April 2014, the Russian Government had responded to these events by occupying and annexing the Ukrainian peninsula of Crimea, as well as military intervention in eastern Ukraine, where hostilities continue to this day.

From the start of its Crimean operation, the Russian army moved to gain control of the peninsula's telecommunications infrastructure, severing cables and routing calls through Russian mobile operators. Ukrainian media companies lost their physical assets in Crimea, and local television programming shifted from Ukrainian to Russian channels. With physical access to its control infrastructure, Russia also commandeered the Ukrainian national satellite platform *Lybid*.

> *From the start of its Crimean operation, the Russian army moved to gain control of telecommunications infrastructure.*

In Kyiv, as soon as the Russian military occupied Crimea, the internal security staff of one of Ukraine's largest mobile operators immediately demanded the severing of communications links between Ukraine and the occupied territory. However, its pro-Russian management refused, and maintained unrestricted connectivity as long as possible, likely so that Russian security services could retain access to its internal systems, for intelligence gathering and other information operations.

Ukrainian mobile operators saw an increase in the volume of cyber crime emanating from Crimea, and it is likely that Russian security services acquired intelligence from information collected in this way.

Pro-Russia media, discussion forums, and social network groups were active in propaganda dissemination. The Crimea campaign was even buttressed by mass changes in *Wikipedia*, where Russian propaganda teams altered articles related to the events taking place there.

Today in Crimea, Russian authorities have implemented content filtering for internet access, including the censorship of Ukrainian news sites. In November 2014, Russia announced it would create a cyber warfare-specific military unit in Crimea.

Pro-Ukrainian hackers have attacked Crimean websites during the occupation, such as that of the Crimean Parliament[7] and a site linking to public web cameras.[8] They have also released allegedly official Russian documents related to the conflict which were claimed to be stolen from Russian government servers.[9]

As the conflict shifted to Donbass, cyberspace played an increasingly important role in military operations. Physical attacks destroyed cabling, broadcast infra-

7 'Vulnerabilities in www.rada.crimea.ua',12 March 2014, *Websecurity* http://websecurity.com.ua/7041/.
8 'Ukrainian Cyber Army: video intelligence', *Websecurity* April 23, 2015, http://websecurity.com.ua/7717/.
9 Aric Toler. 'Russian Official Account of Attack on Ukraine Border Guards', *bellingcat*, 30 May 2015 https://www.bellingcat.com/news/uk-and-europe/2015/05/30/russian-official-account-of-attack-on-ukraine-border-guards/.

structure, and ATM networks, and this served to isolate the region from Ukrainian media, communications, and financial services.[10] Military operations were coordinated with propaganda disseminated on Russian TV channels and internet-based media. Finally, the occupation army performs regular forensics checks on computers and mobile devices owned by the population in eastern Ukraine.

Russian signals intelligence (SIGINT), including cyber espionage, has allowed for very effective combat operations planning against the Ukrainian army. Artillery fire can be adjusted based on location data gleaned from mobile phones and Wi-Fi networks.[11] GPS signals can also be used to jam aerial drones. Ukrainian mobile traffic can be rerouted through Russian GSM infrastructure via a GSM signalling level (SS7) attack;[12] in one case, this was accomplished through malicious VLR/HLR updates that were not properly filtered. Russian Security Services also use the internet to recruit mercenaries.

> *Russian signals intelligence (SIGINT) has allowed for effective combat operations against the Ukrainian army.*

Generally speaking, the computer systems and mobile communications of Ukrainian government, military, and critical infrastructure are under permanent attack, and their communications are routinely intercepted and analysed for information of intelligence value. There are also many attacks on Ukrainian businesses: examples include the Ukrainian Railway Company, Kievstar mobile operator,[13] a SMART-TV retail shop,[14] and a city billboard.[15]

4 Cyber Tactics

Cyberspace is a complex domain. In the Ukraine conflict, we have seen many different types of actors, tools, and tactics. Hacktivists have used the Low Orbit Ion Cannon; criminals have used malware like Blackenergy and DirtJumper. But with cyber attacks, attribution and motive are not always clear, and the level of deception is high. The pro-Russia hacker groups Cyberberkut and Cyber-riot Novorissia have conducted DDoS attacks and released stolen email and office documents from Ukrainian officials. Russian media, parliament members, and pro-Russian

10 Some attacks against telecom infrastructure took place in Kyiv as well.

11 'In the area of ATO proposes to ban military use mobile phones', Голос *України*, 12 May 2015 http://golosukraine.com/publication/zakonoproekti/parent/41516-u-zoni-ato-proponuyut-zaboroniti-vijskovim-koristu/#.VYbMdnWlyko.

12 'How the Russians attacked Ukrainian mobile operators', *Delo.ua*, 26 May 2014, http://delo.ua/tech/kak-rossijane-atakovali-ukrainskih-mobilnyh-operatorov-237125/.

13 Kyivstar is owned and controlled by Russian business, so this attack may be from a non-Russian actor.

14 The TV's firmware was compromised, after which the TV began to display channels from of pro-Russian, separatist eastern Ukraine.

15 The billboard then displayed pro-Russian messages.

Ukrainian politicians often mention these groups by name, but true attribution is difficult. For example, spam is used to deliver news about their operations.[16]

For DDoS, various types of network flooding have been used against web and DNS servers from spoofed source IPs.[17] Sometimes, the attacks overwhelmed internet channel bandwidth; at other times, they affected the capability of an internet router to process packets. The offending bots were located all over the world, but when Ukrainian ISPs began to filter traffic based on national IP ranges, the point of attack simply shifted to Ukrainian bots, which served to defeat this protection measure. During the revolution in Ukraine, DDoS attacks lasted up to weeks at a time, which had never been seen before. Cloud DDoS protection services provided some relief, but the attackers could usually find some worthwhile computer to shut down, such as when they blocked updates to an online media portal.

> *DDoS attacks lasted up to weeks at a time, which had never been seen before.*

Over time, computer security companies have improved their ability to place malware into 'families' and attacks into 'campaigns'. To some degree, this helps to provide attribution, especially when some sophisticated, persistent campaigns can only be the work of nation-state actors – for reasons of mission focus, cost, and the overall level of operational effort required.

Researchers believe, for example, that the Ouroboros/Snake malware family, which avoided detection for 8 years and actively targeted the Ukrainian Government, has Russian origins.[18] With enough data, it is possible to see large cyber espionage campaigns that encompass many different types of targets; it is also possible to see that they generally work within a particular time zone, such as Moscow.[19] One possible Russia-based campaign against Ukraine (and other nations), called Sandworm, exploits advanced 'zero-day' vulnerabilities and targets national critical infrastructure.[20] Finally, in 'Operation Armageddon', researchers believe that they tied malware activity to ongoing Russian military operations in Ukraine.[21]

16 Even the pro-Russian NGO 'Mothers of Soldiers,' which fights the mobilization efforts of the Ukrainian army, uses spam to distribute information.

17 The breadth of the attacks included IPv6->IPv4 to bypass DDoS filters, NTP amplification, slow HTTP POST packets against vulnerable Apache servers, DAVOSET, and SSL renegotiation against misconfigured web servers. The maximum volume I am aware of was <30 Gbt/s.

18 David E. Sanger and Steven Erlangermarch, 'Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government', *New York Times*, 8 March 2014, http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyber-attacks-target-ukraines-government.html?_r=0.

19 'APT28: A Window into Russia's Cyber Espionage Operations?' *FireEye*, 27 October 2014, https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.

20 Stephen Ward. 'iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign', *iSIGHT Partners*, 14 October, 2014, http://www.isightpartners.com/2014/10/cve-2014-4114/.

21 Robert Hackett. 'Russian cyberwar advances military interests in Ukraine, report says' *Fortune*, 29 April 2015, http://fortune.com/2015/04/29/russian-cyberwar-ukraine/.

5 Conclusion and Recommendations

Ukraine is vulnerable to Russia, both in traditional geopolitical space and in cyberspace. In 2015, Ukrainians are still dependent on Russian web resources, including social media (*Vkontakte*), email (Mail.ru), search engines (*Yandex*), antivirus software (Kaspersky), and much more. Our IT supply chain acquires hardware that is either produced in Russia or travels through Russia – this creates vulnerabilities out of the box, and facilitates future attacks.

Whereas Russia is a world leader in cyber espionage and attack, Ukraine's security services are new and inexperienced. In the current conflict with Russia, the only option available to Ukraine is simply a self-inflicted denial-of-service: block access to pro-Russian sites, remove access to Russian TV channels, limit the use of Russian hardware and software, ban mobile phone and social network usage for Ukrainian soldiers, and sever network access with occupied eastern Ukraine.

In the future, Ukraine must modernise its cyber security legislation. One critical aspect of that process will be transparency: it must publish proposed and new laws on government websites so that they are easy to read and understand. In the past, even the few websites available were often knocked offline by hackers.

There have been many lessons learned. Here are some of the author's personal recommendations to the Ukrainian Government:

- Clear Ukrainian IP space of botnets and misconfigured servers (NTP, DNS, etc.) that facilitate cyber attacks;
- Remove illegal and pirated software from critical infrastructure and public agencies;
- Reduce Ukraine's IT dependency in the context of crisis scenarios;
- Implement continuity standards for media and telecoms in conflict zones;
- Create mechanisms to reliably deliver messages from the government to its citizens in occupied territories;
- Incorporate anti-DDoS solutions into Internet-facing services;
- Ensure multiple, independent routes for internet traffic between Ukraine and the rest of the world;
- Implement effective filtering mechanisms on national traffic exchange points;
- Develop a culture of continuous cyber attack monitoring, investigation, information sharing, and research;
- Develop strong cyber security and cryptography capabilities across Ukraine;
- Implement effective civil society controls over unauthorised interception and collection of data;
- Improve emergency data erasure and disaster recovery capabilities;

- Provide resources to military and security services to effectively conduct large-scale cyber operations and computer forensics during their missions; and
- Ensure supply chain security for IT services coming from Russia.

Finally, the world should not underestimate Russia, which is seeking to re-establish its former empire, to include Ukraine and other parts of the defunct Soviet Union and Warsaw Pact. In the context of its wide-ranging political and military campaigns, Russia has developed a cyber attack capability that can target national critical infrastructures, via the internet, anywhere in the world.