Cyber Proxies and the Crisis in Ukraine

by
Tim Maurer

Chapter 9 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

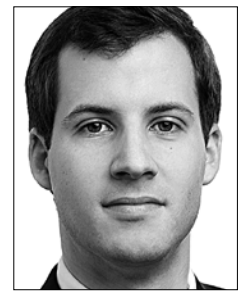
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

In Chapter 9, Tim Maurer of the New America Foundation explores the role that non-state, 'proxy' cyber actors have played in the Ukraine crisis. In both Russia and Ukraine, there is ample private sector computer hacking expertise which each government would theoretically have an incentive to exploit for efficacy and plausible deniability. However, throughout this crisis, there has counterintuitively been very limited proxy use. There have been a few dubious 'hacktivist' attacks, but expert volunteers and cyber criminals do not appear to have been politicised or mobilised to any significant degree in support of geopolitical cyber campaigns. Criminal behaviour remains largely profit-driven. In particular, the Ukrainian Government has not shown a capacity to harness volunteer cyber expertise, as Russia is thought to have done during its previous crises with Estonia and Georgia.

CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Cyber Proxies and the Crisis in Ukraine



Tim Maurer
New America

1 Introduction

In July 2015, I travelled to Kyiv to investigate the role of cyber proxy actors as part of a long-term, global research project on the issue. The Ukrainian crisis seemed like the perfect case study to explore how states use non-state actors and their capabilities. The findings confirmed some of my assumptions but also revealed some surprises. This article outlines what I learned during the trip based on interviews with 11 individuals including current and former government officials, private sector representatives, security researchers, and Eugene Dokukin, the 'commander' of the Ukrainian Cyber Forces, in addition to a review of existing literature.[1]

To start, the crisis in Ukraine has several ingredients that appear to make the use of proxies by a state likely, namely (1) an ongoing hot conflict, fuelling (2) incentives for the state to use proxy capabilities and (3) significant capabilities residing outside of but available to the state. With regard to the second, this includes the general political incentive to be able to claim plausible deniability as well as incentives for the state to augment its own capabilities by adding those provided by non-state actors.

It is also helpful to distinguish between two dimensions when analysing proxy actors to ensure greater analytical clarity. First, analysing proxy actors is part of the broader academic inquiry into the governance of violence best described by the title

1 'Cyber warrior steps up effort to help in war with Russia,' *KyivPost*, February 10, 2015, http://www.kyivpost.com/content/kyiv-post-plus/cyber-warrior-steps-up-effort-to-help-in-war-with-russia-380184.html?flavour=mobile.

of Deborah Avant's seminal book *The Market for Force – The Consequences of Privatizing Security*. In that book, Avant investigates the market for force and the role of public and private actors including proxies.[2] The second, narrower dimension focuses on proxy actors used 'to commit internationally wrongful acts using ICTs'.[3] This is the language used in the most recent report of the Group of Governmental Experts (GGE) that is leading the international community's global cybersecurity norms effort under the auspices of the United Nations. Unlike the first dimension which examines proxy actors more broadly including those that are used by states for defensive purposes, this second lens is about proxy actors used to cause harm to another party.

This short chapter will look at both private actors involved in the general provision of security for the benefit of the state, and private actors using force against a third party to the benefit of the state, but will focus on the latter. The first section outlines in greater detail the conditions present in the region assumed to contribute to the existence of proxy actors. The second part describes the proxy actors that are publicly known to have been active during the crisis.

2 The Making of a Hot Conflict

The hot conflict between Ukraine and Russia was the result of simmering political tension that escalated in November 2013, when former Ukrainian president Viktor Yanukovych abandoned plans to sign a trade agreement with the EU. Yanukovych's decision incited mass protests that were met with a violent government crackdown. In November, long before Yanukovych's flight in February and the build-up of Russian troops on the Crimean border, reports emerged that Russian hacker groups were executing Distributed Denial of Service (DDoS) attacks and defacing websites critical to the Yanukovych government's relationship with Russia. This period was characterised by low-level hacking targeting highly visible websites, either rendering them unavailable or changing their content.

> *Long before Yanukovych's flight, Russian hacker groups were executing DDoS attacks and defacing websites.*

On February 28, shortly after Yanukovych left the country, unmarked soldiers, that Russia's President Putin later acknowledged[4] to be Russian troops, seized a military airfield in Sevastopol and Simferopol international airport. Concurrently, armed sol-

2 'The Market for Force The Consequences of Privatizing Security,' Cambridge University Press, 2005, http://www.cambridge.org/US/academic/subjects/politics-international-relations/comparative-politics/market-force-consequences-privatizing-security.

3 United Nations, General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*,United Nations, July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

4 'Vladimir Putin admits for first time Russian troops took over Crimea, refuses to rule out intervention in Donetsk,' *National Post*, April 17, 2014, http://news.nationalpost.com/news/world/vladimir-putin-admits-for-first-time-russian-troops-took-over-crimea-refuses-to-rule-out-intervention-in-donetsk.

diers tampered with fibre optic cables, raiding the facilities of Ukrainian telecom firm *Ukrtelecom*, which stated afterward that it had 'lost the technical capacity to provide connection between the peninsula and the rest of Ukraine and probably across the peninsula, too'.[5] In addition, cell phones of Ukrainian parliamentarians were hacked and the main Ukrainian government website was shut down for 72 hours after Russian troops entered Crimea on March 2. Patriotic Ukrainian hacker groups such as 'Cyber Hundred' and 'Null Sector' retaliated with DDoS attacks of their own against websites of the Kremlin and the Central Bank of Russia.[6] The day before the presidential election, Ukraine's Security Service (SBU) discovered malware in the systems of the Central Election Commission designed to compromise data collected on the results of the election, revealing how close Russian hackers had come to sabotaging the results.[7] The hacker group 'Cyber Berkut' claimed responsibility.[8]

3 Incentives for the State to Use Capabilities in Private Hands

A general political incentive for states to use proxies is summed up by the concept of 'plausible deniability'. Developed in the context of maritime privateering, it was:

Political incentive for states to use proxies is summed up by the concept of 'plausible deniability'.

> *'invented [by state rulers] at the turn of the seventeenth century. If a 'private' undertaking that a ruler authorised met with success, s/he could claim a share in the profits. If the enterprise caused conflict with another state, the ruler could claim it was a private operation for which s/he could not be held responsible'.*[9]

While some of the specific elements of maritime privateering are no longer relevant today, the general concept and logic for this type of behaviour still apply and exist today. For example, the Russian Government denied any involvement in the Ukrainian crisis for many months, in spite of eyewitness accounts and news reports plainly stating otherwise. One particularly horrible example of plausible deniability was the mass murder of the passengers on Malaysia Airlines flight 17.

The benefits of plausible deniability also apply to the Ukrainian Government. The Ukrainian Cyber Forces, led by Eugene Dokukin, is a volunteer group that

5 'Feb. 28 Updates on the Crisis in Ukraine,' *The New York Times News Blog*, February 28, 2014, http://thelede.blogs.nytimes.com/2014/02/28/latest-updates-tensions-in-ukraine/?_r=0.

6 'Kremlin website hit by 'powerful' cyber attack,' *Reuters*, March 14, 2014, http://www.reuters.com/article/2014/03/14/us-russia-kremlin-cybercrime-idUSBREA2D16T20140314.

7 'Cyber-attack' cripples Ukraine's electronic election system ahead of presidential vote,' RT, 24 May, 2014, http://www.rt.com/news/161332-ukraine-president-election-virus/.

8 'Ukraine election narrowly avoided 'wanton destruction' from hackers (+video),' *The Christian Science Monitor*, June 17, 2015, http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

9 Janice Thomson. *Mercenaries, Pirates, and Sovereigns* (Princeton, NJ: Princeton University Press, 1994), 21.

occasionally publishes data from the Russian Ministry of the Interior, and at one point threatened to shut down the internet in the Crimea and other cities in eastern Ukraine.[10] There is no evidence suggesting that the Ukrainian Government coordinates or directly supports any of the Ukrainian Cyber Forces' activities, and my own research supports this conclusion. At the same time, the Government benefits from its activities with or without its involvement. For the Ukrainian Government, another set of incentives is arguably more important than the political ones: its own limited capabilities, and the possibility to rely on proxy actors to augment these capabilities in the face of a much more powerful opponent.

The Russian Government is considered to be among the most sophisticated actors with significant in-house cyber capabilities,[11] and the government in Ukraine faced a dire situation at the beginning of the conflict. Its military had essentially been falling apart since the end of the Soviet Union and Kyiv was ill-prepared for a conflict with Russia. As Dmitry Gorenburg points out:

> *'At the time of its creation, the Ukrainian military was considered the fourth most powerful conventional military force in the world, behind only the United States, Russia, and China. However, these forces were allowed to atrophy throughout the post-Soviet period, with virtually no funding provided for the maintenance of equipment or troop training. Reforms were not carried out and there were no attempts at rearmament to replace aging Soviet equipment'*.[12]

The responses from several interviewees confirmed this assessment.

4 Capabilities Outside the State

In order for a state to be able to pursue the incentives of using proxy actors, private actor capabilities must exist in the first place. With regard to cyberspace, such capabilities include those present within a state's territory and beyond. Regarding the former, significant capabilities have been present in Ukraine and Eastern Europe since the 1980s. Misha Glenny, the award-winning journalist, recounts in his 2011 book *Dark Market – How Hackers Became the New Mafia* that:

> *'The hackers of Eastern Europe played a particularly important role in cracking security devices played on software…Bulgaria, Ukraine and Russia set the pace, with the Romanians not far behind.'*[13]

10 'Ukraine's Lonely Cyberwarrior vs. Russia,' *The Daily Beast*, February 18, 2015, http://www.thedailybeast.com/articles/2015/02/18/ukraine-s-lonely-cyber-warrior.html.

11 'Russia Tops China as Principal Cyber Threat to US,' *The Diplomat*, March 3, 2015, http://thediplomat.com/2015/03/russia-tops-china-as-principal-cyber-threat-to-us/.

12 Dmitry Gorenburg. 'Russia and Ukraine: Not the Military Balance You Think,' *War on the Rocks*, November 10, 2015, http://warontherocks.com/2014/11/russia-and-ukraine-not-the-military-balance-you-think/.

13 Misha Glenny. *McMafia: A Journey Through the Global Criminal Underworld* (New York, Vintage Books: 2009), 59; see also Nadiya Kostyuk's chapter in this book.

Ukraine was the cradle of CarderPlanet, which was 'changing the nature of cybercrime around the world'.[14] One explanation why technically skilled people in the region decided to pursue cybercrime to make a living was the lack of other opportunities. For example, a job in the Ukrainian Government for somebody in his 20s pays roughly $3,000 – a year, not a month. And while Samsung has one of its largest R&D centres in Kyiv, the private IT industry is neither large nor attractive enough to absorb all of the skilled labour, unlike in Israel, for example.[15] Interestingly, 'CarderPlanet was penetrated and compromised by the Russian Secret Police almost as soon as it was set up' but:

> *'why would the KGB waste resources on investigating networks that are ripping off American and European credit cards? A complete waste of time. So for the moment, Moscow was content to observe and store information. They knew exactly who was who in the Odessa carding community'*.[16]

Yet, it was not only the FSB that knew what was happening in Eastern European countries. In 2009, Brian Krebs, an expert on cybercrime in the region and widely read not only by law enforcement officials in the U.S. but also Ukraine, wondered:

> *'whether authorities in those countries would be any more willing to pursue cyber crooks in their own countries if they were forced to confront just how deeply those groups have penetrated key government and private computer networks in those regions?'*

An example is Dmitry Ivanovich Golubov, once considered a top cybercrime boss by U.S. law enforcement, but now a leader of the Ukrainian Internet Party participating in parliamentary elections. Russian agencies reportedly provide little assistance with shutting down networks such as the Russian Business Network. Last but not least, cyber criminals also do their best to avoid attracting local law enforcement attention. As Krebs notes:

> *'Some of the most prolific and recognizable malware disbursed by Russian and East European cyber crime groups purposefully avoids infecting computers if the program detects the potential victim is a native resident.'*[17]

In sum, there is no shortage in the region of labour skilled in information technology and hacking, while a mature industry is missing, and government salaries of a few thousand dollars a year pale in comparison to reports of thousands or millions of dollars made in the latest cyber heist.

---

14 Misha Glenny. *McMafia: A Journey Through the Global Criminal Underworld*, 48.

15 'Nearshoring: Top 20 largest In-House R&D offices in Ukraine,'GoalEurope, October 4, 2013, http://goaleurope.com/2013/10/04/nearshore-outsourcing-top-20-largest-rd-offices-in-ukraine/.

16 Misha Glenny. *McMafia: A Journey Through the Global Criminal Underworld*, 52-53.

17 'Story-Driven Résumé: My Best Work 2005-2009,' *KrebsonSecurity*, December 9, 2010, http://krebsonsecurity.com/2009/12/story-driven-resume-my-best-work-2005-2009-3/.

5 Mapping and Analysis of Proxy Actors

There are several important findings regarding proxies and the conflict in Ukraine. The first is that proxy actors are active as part of the conflict in Ukraine. The second is that the amount of cyber proxy activity has remained relatively low. There are two likely explanations for this: there has been a relatively low number of significant cyber incidents associated with the conflict other than during its initial phase as described above; and while there was clearly a significant wave of patriotism and willingness by Ukrainian citizens to volunteer and support the government, several interviewees suggested that the government in Kyiv did not have the ability to absorb and coordinate these extra capacities. In other words, to draw from the political science literature on power, while significant cyber power resources in the hands of private actors existed, the Ukrainian Government was not able to effectively mobilise these resources to actually project power. Kyiv's cyber power was inhibited by a lack of what Alexander Klimburg calls 'integrated national capability'.[18]

Thirdly, the conflict does not appear to have mobilised the most sophisticated non-state actors with cyber capabilities in the region – the cybercriminals – to change their profit-driven behaviour to more politically-driven action. While the conflict apparently politicised and led to a split of the criminal underground community in the autumn of 2014, the effect was ephemeral and once the cybercriminals realised that their spat started to affect their business, 'money trumped politics', according to Konstatin Korsun, head of council at the NGO Ukrainian Information Security Group and director at the private cybersecurity company Berezha Security.[19]

> *Once cybercriminals realised that their spat started to affect business, 'money trumped politics'.*

A closer look reveals a range of proxy actors has been active. In the context of a broader analysis of the market for force, it is notable that the crisis in Ukraine demonstrated that cybersecurity is a domain where private actors possess significant capabilities and are used by states for both defensive and offensive purposes. For example, the limited capabilities of the Ukrainian Government have been augmented through NATO assistance, namely its Cyber Defence Trust Fund, to train and improve Ukraine's cyber defences. Interestingly, the lead NATO member providing that assistance, Romania, has itself not been providing this assistance directly through its government, but is relying on a proxy actor, a state-owned company called Rasirom, to provide the service.[20]

18 Joseph S. Nye, Jr. *The Future of Power* (New York: Public Affairs, 2011).
Alexander Klimburg, 'Mobilising Cyber Power,' *Survival* 53.1 (2011), 56.

19 'Kostiantyn Korsun,' LinkedIn, accessed August 25, 2015, https://ua.linkedin.com/pub/kostiantyn-korsun/1b/12b/580.

20 'Romania Turns Hacking Crisis Into Advantage, Helping Ukraine,' *The New York Times*, May 13, 2015, http://www.nytimes.com/aponline/2015/05/13/world/europe/ap-eu-romania-ukraine-cyber-warfare.html; 'NATO-Ukraine Trust Fund on Cyber Defence,' Romania's Permanent Representation to NATO, accessed August 25, 2015, http://nato.mae.ro/en/local-news/804.

While criminal groups have not been active players in the Ukraine conflict, the most prominent proxy actors have been hacktivist groups. These groups include pro-Kyiv OpRussia, Russian CyberCommand (which considers itself to be part of Anonymous),[21] Cyber Ukrainian Army, Cyber Hundred, Null Sector,[22] and the pro-Moscow CyberBerkut and Anonymous Ukraine.[23] Their activities have been limited to DDoS attacks, web defacements, and the occasional leaking of government files. The most serious incident involved the aforementioned targeting of the Ukrainian voting system during the Ukrainian Presidential election. While Ukrainian government officials and many news reports blame the Russian Government for indirectly orchestrating these operations, as well as for the crude 'hack attacks' on Ukrainian state websites, the Russian Government has vehemently denied accusations that it has any influence over these groups. Evidence for a relationship between pro-Russian separatists or hacker groups such as Cyber Berkut and the Russian Government remains lacking.

The Ukrainian Cyber Force has been among the most prominent Ukrainian hacktivist groups. It is led by Eugene Dokukin and a group of volunteers he recruited through social media, whose number has fluctuated from several dozens to a few hundred, and primarily includes ordinary citizens without a technical background.[24] The Ukrainian Cyber Force combines a series of different activities, ranging from the unauthorised monitoring of CCTV cameras in eastern Ukraine and Russia, to reporting troop and separatist activities to web companies in an effort to shut down their accounts, launching DDoS attacks against websites, and leaking sensitive documents from the Russian Government. While Dokukin has given a series of interviews and shares information about his actions with the media and the government, there is no evidence that the government coordinates or supports him financially or otherwise. Instead, the government has been turning a blind eye.

Related to the conflict in Ukraine are the findings of several industry reports. The U.S.-based security company FireEye published a report titled '*APT28: A Window into Russia's Cyber Espionage Operations?*', detailing the activities of a group conducting political espionage against East European countries and security organisations. FireEye:

> *'conclude[s] that we are tracking a focused, long-standing espionage effort. Given the available data, we assess that APT28's work is sponsored by the Russian Government'*.[25]

21 Jeffrey Carr. 'Rival hackers fighting proxy war over Crimea,' *CNN*, March 25, 2014, http://www.cnn.com/2014/03/25/opinion/crimea-cyber-war/.

22 'Cyber Wars: The Invisible Front,' *Ukraine Investigation*, April 24, 2014, http://ukraineinvestigation.com/cyber-wars-invisible-front/.

23 'Cyber Berkut Graduates From DDoS Stunts to Purveyor of Cyber Attack Tools,' *Recorded Future*, June 8, 2015, https://www.recordedfuture.com/cyber-berkut-analysis/.

24 'Cyber warrior steps up effort to help in war with Russia,' *KyivPost*, February 10, 2015, http://www.kyivpost.com/content/kyivpost-plus/cyber-warrior-steps-up-effort-to-help-in-war-with-russia-380184.html.

25 'APT28 – A Window Into Russia's Cyber Espionage Operations?' *FireEye*, October 27, 2014, https://www2.fireeye.com/apt28.html.

Perhaps the most interesting report is the one published by the Finnish firm F-Secure titled '*BlackEnergy & Quedagh – The convergence of crimeware and APT attacks*'. The authors highlight that in 2014, malware named BlackEnergy, originally developed and used for criminal profit-driven purposes, was deployed against government organisations in Ukraine by a group the report calls 'Quedagh'. The report concludes by stating that:

> *'the use of BlackEnergy for a politically-oriented attack is an intriguing convergence of criminal activity and espionage. As the kit is being used by multiple groups, it provides a greater measure of plausible deniability than is afforded by a custom-made piece of code.'*[26]

6 Conclusion

The conflict in Ukraine includes a range of proxy actors and proxy activity. This should be expected given the existence of a hot conflict, the presence of significant cyber capabilities in private hands, and incentives for the nations involved to use these private capabilities. However, the amount of cyber proxy activity has remained relatively low, much like the overall level of computer network operations compared to what some experts predicted. It is notable that the conflict does not appear to have politicised and mobilised the most sophisticated non-state actors with cyber capabilities – the cybercriminals – to change their profit-driven behaviour to more politically-driven action. Moreover, the Ukrainian Government has not had the capacity and strategy in place to be able to absorb the additional capabilities provided by volunteers. Kyiv has therefore not been able to mobilise and project the full potential of Ukraine's power due to the limited use of its true power resources. While the Ukrainian Government regularly accuses the Russian Government of using proxies, there seems to be less vehemence from the Russian side criticising, for example, the activities of the Ukrainian Cyber Forces. According to one interviewee, one explanation is that the Russian Government has more to gain from being able to point to the existence of Ukrainian proxies in order to thereby indirectly legitimise the existence of Russian proxies.

While this chapter hopefully shed some light on the role of proxy actors in the Ukraine conflict, it is necessary to point to some important limitations and issues that were beyond the scope of this short piece. First, the term 'proxies' lacks a clear definition. While it is used in the GGE report, it is not defined, even though the report distinguishes 'proxies' as a separate type of actor from state and non-state actors. Developing a more systematic and nuanced analytical framework for proxies is therefore the focus of my current research. This will hopefully be useful for future empirical research on proxy actors around the world, as well as for ongoing policy discussions through the GGE and elsewhere.

26 'The convergence of crimeware and APT attacks,' *F-Secure*, 2014, https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.