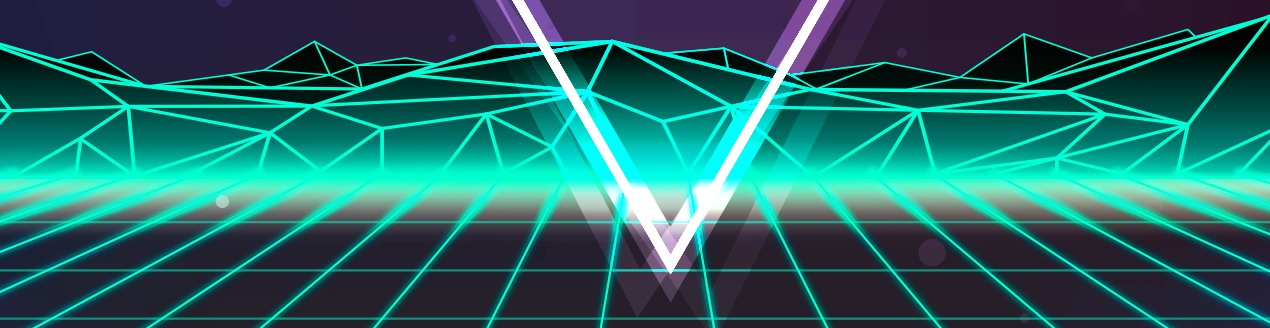
# Introduction: Cyber War in Perspective

by

Kenneth Geers



Chapter 1 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

# Introduction: Cyber War in Perspective

Kenneth Geers

*NATO CCD COE*[1] */ Atlantic Council /*
*Taras Shevchenko National University of Kyiv*

Cyber war is a hot topic. Armed forces, intelligence, and law enforcement agencies have made computer security – from defence to offence – a top priority for investment and recruitment. In fact, current efforts to take the higher ground in cyberspace are so intense that many governments will overreach, with unfortunate ramifications for democracy and human rights around the world.

The current Russo-Ukrainian conflict appears to have all the necessary ingredients for cyber war. Moscow and Kyiv, and indeed the entire NATO Alliance, are playing for the highest geopolitical stakes. Russia has already annexed Crimea, and there is an ongoing military standoff in eastern Ukraine. Both countries possess a high level of expertise in science, technology, engineering and mathematics (STEM), which has naturally led to an aptitude for, and experience with, computer hacking.

Despite these factors, there are still many sceptics over cyber war, and more questions than answers. Although malicious code has served criminals and spies very well, can cyber attacks offer soldiers more than a temporary, tactical edge on the battlefield? Can it have a strategic effect? What norms should be established in international relations to govern nation-state hacking in peacetime and in war?

> *Can cyber attacks offer soldiers more than a temporary, tactical edge on the battlefield?*

1 Dr Kenneth Geers was a Scientist at NATO CCD COE in 2007–2011 and now holds the position of Centre Ambassador.

This book serves as a benchmark in the early history of Internet-era warfare. For world leaders and system administrators alike, the 'cyber dimension' of the Ukraine crisis offers many lessons and sheds light on whether cyber war is still closer to science fiction than reality. The research is divided into five sections: Strategic Framework, Tactical Viewpoints, Information Warfare, Policy and Law, and The Future. Each chapter has been written by a leading expert in national security, network security, or both. It has been a pleasure and an honour to work with all of them. Many thanks to the North Atlantic Treaty Organisation Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) for sponsoring this research.

*Cyber War in Perspective: Russian Aggression against Ukraine* opens with a chapter by Russia scholar **Keir Giles** of the Conflict Studies Research Centre in Oxford, UK. Keir offers deep insight into the background to this crisis, and explains why it may not be resolved any time soon. Russia and the West are said to have two distinct views of the world. Moscow is unlikely to tolerate true independence and sovereignty for its former Soviet satellite states, and remains vehemently opposed to Western support for them. It has many strategies and tactics – traditional and cyber – that it can employ against Ukraine and its other neighbours, while the West is both hesitant and divided.

In Chapter 3, **James J. Wirtz**, Dean of the Naval Postgraduate School in California, describes the global context surrounding these events. Today, nation-states are integrating cyber tactics into their political and military strategies. Professor Wirtz posits that when it comes to the use of cyber, 'national styles' might be emerging as states attempt to use cyber capabilities to achieve strategic objectives. He suggests that it is wrong to treat cyber attacks as a silver bullet, and that it is better to consider how a sort of combined arms approach will prevail. On a positive note, the need for legal and bureaucratic integration of policies and programmes should produce national idiosyncrasies on the cyber battlefield that can help with the vexing challenge of attribution.

**James Andrew Lewis** of the Centre for Strategic and International Studies (CSIS) analyses the geopolitical effects of cyber attacks in Chapter 4. He discusses two metrics: strategic effects that diminish an opponent's will or capacity to fight (e.g. influencing public opinion) and tactical effects that degrade military power (e.g. confusing troops, or denying service to weapons). Success is premised upon observable, real-world effects. In Ukraine, Russian cyber operations had no strategic effect and only a limited, short-term political effect.

In Chapter 5, RAND's **Martin Libicki** takes one of this book's strongest stances. He asks why, despite the existence of a hot military conflict and ample hacker talent, there is *no cyber war* in Ukraine. There have been hacktivist outbursts, web defacements, distributed denial-of-service (DDoS) attacks, and cyber espionage, but everything we have seen so far falls well short of how national security thinkers – and Hollywood – have portrayed cyber war. Libicki explores several possible reasons. Does Ukraine not possess cyber-enabled critical infrastructures? Are Russia

and Ukraine wary of taking (or escalating) their conflict into the cyber domain? Or are our notions of cyber war simply overrated?

**Nikolay Koval**, head of Ukraine's Computer Emergency Response Team (CERT-UA) during the revolution, describes in Chapter 6 how cyber attacks rose in parallel with ongoing political events, in both number and severity. In 2012, hackers 'defaced' Ukrainian government websites with politically motivated digital graffiti. In 2013, network defenders discovered new and more menacing forms of malware, such as RedOctober, MiniDuke, and NetTraveler. In 2014, hacktivist groups such as *CyberBerkut* published stolen Ukrainian Government documents. Koval analyses in detail the most technically advanced attack investigated by CERT-UA: the May 2014 compromise of Ukraine's Central Election Commission (CEC). He closes by appealing to the Ukrainian Government to allocate greater funds to hire and retain qualified personnel.

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.

FireEye's **Jen Weedon**, in Chapter 8, discusses Russia's strategic use of computer network exploitation (i.e. cyber espionage). Today, via the Internet, intelligence agencies can gather information on an industrial scale, which can be used for any purpose, including tactical support to military operations. From a targeting perspective, Weedon discusses strategies for creating a decisive information advantage, 'prepping' a battlefield through denial and deception, and how hackers might even cause real-world physical destruction; and details the technical aspects of suspected Russian cyber operations, including malware samples, hacker tactics, and compromised infrastructure.

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.

Swedish Defence University researcher **Margarita Levin Jaitner** highlights current Russian Information Warfare (IW) theory in Chapter 10. She contends that Moscow has an inherent belief in the power of information control to advance its political and military goals. In Russian doctrine, cyber security is subordinate to information security, and cyberspace is only one part of the 'information space'. National security planners are concerned with both 'technical' and 'cognitive' attacks, and recognise that achieving information superiority involves everything from propaganda to hacking to kinetic military operations. Margarita Jaitner argues that the annexation of Crimea was a textbook case in information superiority.

> *Moscow has an inherent belief in the power of information control.*

In Chapter 11, **Liisa Past**, a NATO CCD COE expert on strategic communications, analyses leadership discourse. Liisa Past reveals that Russian President Vladimir Putin and Ukrainian President Petro Poroshenko have employed similar rhetorical strategies, including the development of an 'us vs. them' dichotomy in which the in-group is portrayed as constructive and solution-oriented, while the out-group is illegitimate and dangerous. In their current conflict, neither Russia nor Ukraine denies that cyberspace is a domain of warfare, but neither has stressed its importance. Russian political discourse has mostly overlooked cyber issues (which is in line with Russian military doctrine), while Ukraine has framed them within the larger concept of 'hybrid warfare'. The most notable difference in political rhetoric is Kyiv's clear orientation to the West and NATO, while Moscow is keenly focused on Russian national interests.

**Elina Lange-Ionatamishvili** and **Sanda Svetoka** of the NATO Strategic Communications Centre of Excellence in Latvia, in Chapter 12, discuss the role of social media in this conflict. In the Internet era, the battle for hearts and minds has never been more important. Social media is a trust-based network that provides fertile soil for intelligence collection, propaganda dissemination, and psychological operations (PSYOPS) to influence public opinion – or to lead adversaries into harm's way. 'Soft' cyber attacks can be as severe as any attack on critical infrastructure. In Ukraine, they have generated fear, uncertainty, and doubt about the economic, cultural, and national security of Ukraine, while promoting positive messages about Russia's role in Crimea and eastern Ukraine. The authors provide recommendations for defence against such attacks, including how to identify them, challenge them, and how to develop a resilient political narrative to withstand false propaganda.

In Chapter 13, University of Michigan doctoral student **Nadiya Kostyuk** reviews Ukraine's cyber security policy – past, present, and future. She analyses numerous historical factors that make Ukraine a cyber safe haven: a strong science, technol-

ogy, engineering, and mathematics (STEM) education, underwhelming economic performance since the fall of the Soviet Union in 1991, and social norms which dictate that stealing from the West is not a bad thing. The icing on the cake is that there are currently few cyber security regulations in Ukraine. All of these factors shed light on the vexing challenge of containing cyber crime in the region. Looking toward the future, Nadiya Kostyuk argues that Ukraine's political, military, and economic crises will inhibit the stabilisation of Ukrainian cyberspace for some time.

Lt Col **Jan Stinissen** of the NATO CCD COE, in Chapter 14, offers a legal framework for cyber operations in Ukraine. He explains that international law applies to cyberspace, and the law of armed conflict applies to all relevant cyber operations. Jan discusses the legal definitions of 'war' and 'cyberwar', as well as the concepts of 'armed conflict', 'armed attack', and 'use of force'. Typically, cyber attacks do not come in isolation, but rather as one element of a larger military operation; the wider context will determine the legal framework for its cyber component. There are many qualifying factors including state vs. non-state actor, and armed conflict vs. law enforcement. In the Ukraine crisis, operations in Crimea (which has already been annexed by Russia) may be viewed differently from those in eastern Ukraine. Stinissen asserts that, globally, most known cyber attacks have simply not been serious enough to be governed by the law of armed conflict, but that this is likely to change in the future.

In Chapter 15, NATO CCD COE researcher **Henry Rõigas** discusses the impact of known cyber attacks in Ukraine on proposed political cyber 'norms', the rules of state behaviour in international relations. On the positive side, the absence of attacks against critical infrastructure could be a boon to future international security and stability, especially if it is a result of intentional restraint on the part of Moscow and Kyiv. This case challenges the prevailing perception that a loose normative framework currently allows states to employ cyber attacks as a tool for coercion. On the negative side, the examples of computer network operations we have seen appear to violate the information security norms promoted by Russia and the Shanghai Cooperation Organisation (SCO), as they seem to constitute a war on information itself, that is a dedicated effort to alter public opinion through deceptive propaganda.

Finnish Professor **Jarno Limnéll**, in Chapter 16, discusses the ramifications of the Ukraine war, and its cyber component, for Russia's neighbours. Moscow's aggressive behaviour in Ukraine has forced many countries to re-evaluate their political and military relationships, especially with NATO. For historical reasons, Finland and Estonia are well positioned to analyse Russia's use of hybrid warfare, including information operations. Today, these countries are actively pursuing ways to bolster their national defences against Russia's military strategies and tactics in Ukraine. The NATO Alliance should take concrete measures to reassure its member states, such as the creation of a common cyber defence framework.

In Chapter 17, **Jason Healey** and **Michelle Cantos** of Columbia University imagine four potential cyber conflict scenarios in this crisis. First, even if the hot

war cools off, Russia can still raise the temperature in cyberspace, and cause serious network disruptions in Ukraine. Second, Russia could selectively target the West, adding a new vector to its already increased volume of threats, military exercises, submarine deployments, and nuclear warnings. Third, Vladimir Putin could mirror the 'frozen conflict' dynamic in cyberspace by threatening prolonged disruptions of the global Internet. And fourth, if the Ukraine conflict spins out of control, Russia, in desperation, might even have the power to take down the Internet entirely.

*Hostile nation-state cyber operations are a long-term, dynamic, multidimensional threat.*

To close our book, in Chapter 18, Brookings Institution Nonresident Senior Fellow **Richard Bejtlich** offers essential advice not only for Ukraine, but for any nation or organisation wishing to improve its cyber security posture. Bejtlich draws from the deep well of classic military doctrine, arguing that hostile nation-state cyber operations are not a single event but a long-term, dynamic, multidimensional threat. The only hope that Ukraine or any other nation has for building an effective defence against professional network attacks is to incorporate strategic thinking into its defensive architecture, personnel, and operations.