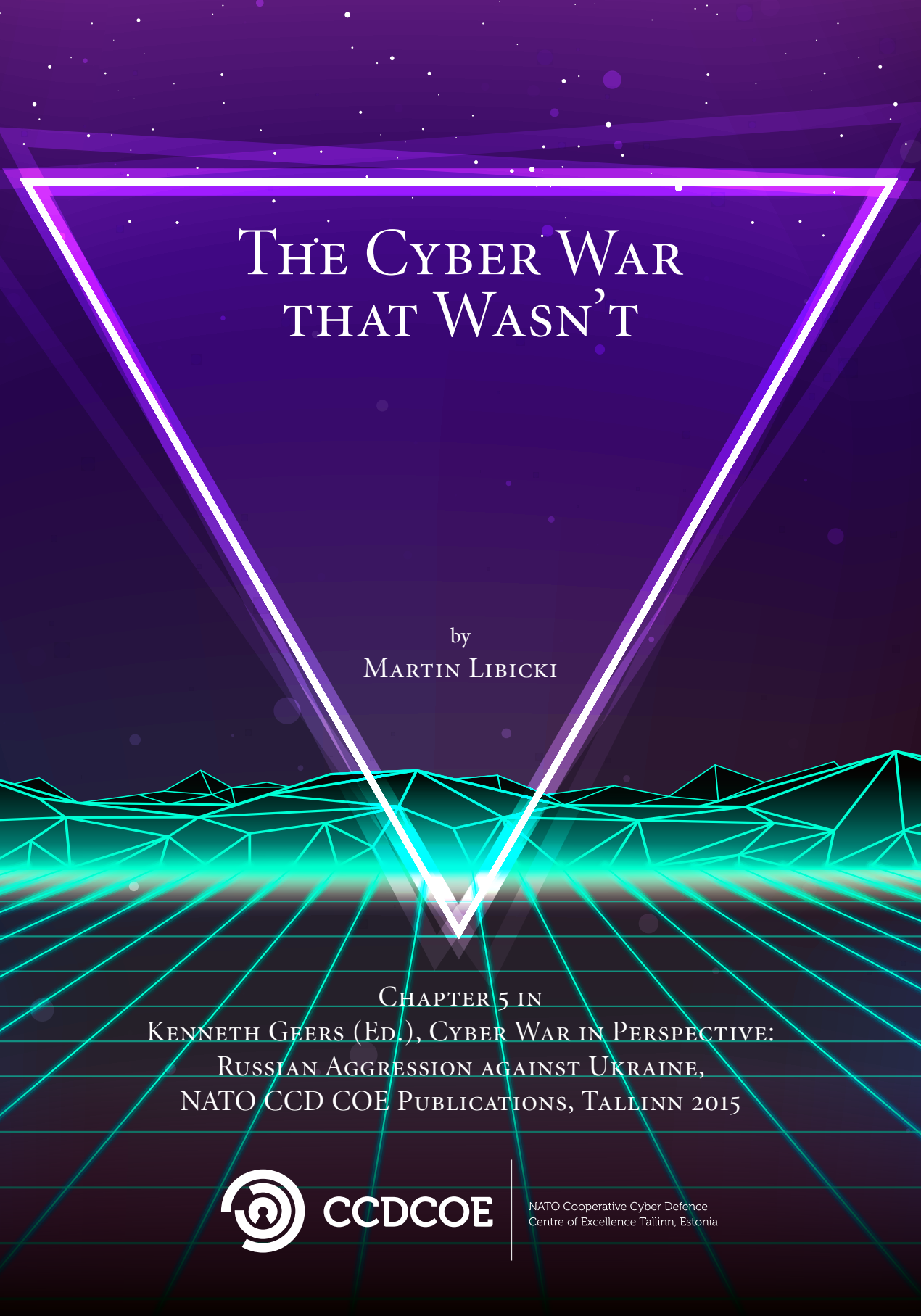


The Cyber War that Wasn't

by

Martin Libicki

Chapter 5 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

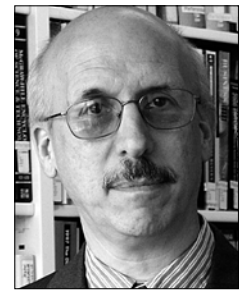
CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

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?

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

The Cyber War that Wasn't



Martin Libicki
RAND

1 Introduction: Isn't It Time for Cyber War?

For the last twenty years, with the advent of serious thinking about 'cyber war', most analysts – and even the more sceptical thinkers – have been convinced that all future kinetic wars between modern countries would have a clear cyber component. However, the current Russo-Ukrainian conflict is challenging this widely held notion.

Coinciding with this assumption, however, it must be said that within the past generation there have been few conflicts in which both sides appeared both capable of and vulnerable to cyber attack. Either one party to the conflict – usually the United States – held all the cyber cards, or neither did. For cyber war to take place, at least one side must have enough digitised networked equipment to make much difference. In some past conflicts, the US may have abstained from firing digital weapons because the other side simply lacked appropriate targets. Many analysts have speculated that the US, and now other highly networked societies, may hesitate to use cyber tactics because of their own inherent vulnerabilities in this domain.

> *Analysts have been convinced that future kinetic wars would have a clear cyber component.*

Apart from Stuxnet, the most frequently cited example of cyber war in action came during an alleged Israel Air Force strike against Syrian nuclear facilities in 2007. Integrated air-defence systems (IADS) have been considered ripe targets for

cyber warfare, but it was understood that there would be a cost-benefit analysis relative to dispatching them using more familiar tools such as electronic warfare or missiles. There were rumours, for example, that the US employed cyberwar techniques against Serbian IADS in 1999, but these rumours were never substantiated. Even the Syrian story may be a fairy tale, as the details are classified and subject to much speculation. It is possible that the tactics were in fact more conventional, such as traditional jamming.[1]

2 Unique Aspects of the Russo-Ukrainian Conflict

The current Russo-Ukrainian conflict, however, is a different case, and it should help us to understand if cyber war is, in 2015, more myth or reality. According to the prevailing assumption, this war should have seen serious and open cyber war strategies and tactics. Both countries have technologically advanced societies and weaponry that at least came up to 1990 standards of modernity. Both countries have a strong information technology (IT) base, and hackers a-plenty, although many of them are engaged in organised crime rather than working for the state.[2] Russia's state-sponsored hackers are widely believed to be on par with, or very close to, NSA-level standards.

The most notable thing about the war in Ukraine, however, is the near-complete absence of any perceptible cyber war. There has been vigorous cyber espionage,[3] the targeting of cell phones by Russian electronic warfare, and the use of old-fashioned bolt-cutters to sever lines of communication in Crimea.[4] Patriotic hacktivists on both sides have conducted harassing but small cyber attacks against each other,[5] both sides have conducted Distributed Denial-of-Service (DDoS) attacks (e.g., by Russia against Ukraine's parliament),[6] and

1 As Richard Clarke and Robert Knake maintain in *Cyberwar, The Next Threat to National Security and What to do About It*, New York NY: HarperCollins, 2010; see also David Makovsky. 'The Silent Strike: How Israel bombed a Syrian nuclear installation and kept it secret,' *The New Yorker,* 17 September 2012, http://www.newyorker.com/magazine/2012/09/17/the-silent-strike.

2 Ukraine's hackers do not make as much news but consider Dan Goodin. 'Strange snafu hijacks UK nuke maker's traffic, routes it through Ukraine,' *ARS Technica UK,* 13 March 2015, http://arstechnica.com/security/2015/03/mysterious-snafu-hijacks-uk-nukes-makers-traffic-through-ukraine/.

3 Apparently, the Russians have developed some powerful malware for that purpose against Ukraine: cyber-snake (aka Ouroboros). See Sam Jones. 'Cyber Snake plagues Ukraine networks,' *FT Online*, 7 March 2014, in http://www.ft.com/cms/s/0/615c-29ba-a614-11e3-8a2a-00144feab7de.html or David Sanger and Steven Erlanger, 'Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government' *NY Times Online*, 8 March 2014, http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html.

4 Sam Jones. 'Kremlin alleged to wage cyber warfare on Kiev,' *FT Online,* 5 June 2014, http://www.ft.com/intl/cms/s/0/e504e278-e29d-11e3-a829-00144feabdc0.html#axzz3b4c6egXI. See also the claim of General Breedlove, EUCOM's Commander: 'They disconnected the Ukrainian forces in Crimea from their command and control,' from Michael Gordon. 'NATO Commander Says He Sees Potent Threat From Russia,' *NY Time Online*, 2 April 2014, http://www.nytimes.com/2014/04/03/world/europe/nato-general-says-russian-force-poised-to-invade-ukraine.html.

5 "Cyber Berkut' Hackers Target Major Ukrainian Bank,' *The Moscow Times*, 4 June 2014, http://www.themoscowtimes.com/business/article/cyber-berkut-hackers-target-major-ukrainian-bank/502992.html of July 4, 2014.

6 Nicole Perloth. 'Cyberattacks Rise as Ukraine Crisis Spills to Internet,' *New York Times Bits*, 4 March 2014, http://bits.blogs.nytimes.com/2014/03/04/cyberattacks-rise-as-ukraine-crisis-spills-on-the-internet/.

a (fruitless) campaign to corrupt voting processes in Ukraine.[7] However, we have seen nothing comparable to the cyber attacks carried out against Estonia in 2007 or Georgia in 2008.

On the other hand, the information and propaganda war in the social media domain (particularly from the Russian side) has been relentless. In this regard, Moscow has a competitive advantage over Kyiv. The two countries share a common language, Russian (the use of the Ukrainian language is growing fast, but that language is Slavic), and most Russian-language-friendly sites such as *VKontakte* (the Russian Facebook) are headquartered in Russia. That said, little if any of the conflict taking place in social media requires subverting computers through the discovery of vulnerabilities or the engagement of exploits.

In particular, there are two major forms of cyber attack that have not taken place in the Russo-Ukrainian conflict: attacks on critical infrastructure and attacks on defence systems. It is possible that, in the future, we may learn that there have been such attacks, but that they were simply subtle enough to slip under the radar. With Stuxnet, Iran's centrifuge plant at Natanz was infected for six months, with centrifuges failing at unexpected rates, before Iranian engineers understood why. Successful cyber attacks could indefinitely be ascribed to incompetent management before a complete picture is understood. And as for military systems, credible stories of their successful attacks may emerge years later, when people are freer to talk about what happened in the war.

Two major forms of cyber attack have not taken place: on critical infrastructure and on defence systems.

Even with all of that in mind, in the Internet era it has become difficult to keep secrets for long periods of time, and the growing absence of cyber attack evidence is turning into the evidence of absence.

3 Possible Reasons for the Absence of Cyber Conflict

So, based on what we know now, why has this kinetic conflict seen so little cyber conflict? Here are some possible answers to that question.

Ukraine does not have the requisite hackers. Russian hackers need no introduction. They work for the state, for cyber crime syndicates, and for themselves as patriotic hacktivist defenders of Mother Russia. However, on the Ukrainian side (a much smaller nation to begin with), it is possible that a large percentage of the hacker talent is of Russian descent and may have divided loyalties in this conflict. That said,

7 Mark Clayton. 'Ukraine election narrowly avoided 'wanton destruction' from hackers,' *Christian Science Monitor,* 17 June 2014, http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

many small countries have made large contributions in cyberspace, including Estonia, Iceland, Lebanon[8] and Israel.

Neither Russia nor Ukraine has valid targets. This gets closer to the truth. Although the Soviet Union of 1990 had sophisticated weapons, their long suits were in metallurgy and radio-frequency devices. When the Soviet Union collapsed, it was significantly behind the West in terms of electronics and software. In the last five years, there has been a modest recapitalisation in Russia, but close to none in Ukraine. Since the end of the Cold War, the United States has for the most part maintained its substantial lead over Russia in digitisation and networking. Thus, US fears about its systems falling prey to hackers are currently not shared by the majority of nation-states, who feel that they are not particularly vulnerable. However, the truth probably lies somewhere in the middle: for example, no one is buying analogue telecommunications systems anymore, not even in the developing world. New equipment is digital and networked, not only because it is more powerful, but because it is cheaper over the long run. Therefore, even in Russia and Ukraine, the level of digitisation is likely high enough to engender real concerns about their societies' vulnerability to cyber attack. Their militaries may be antiquated, but due to the close relationship between the IT of modern civilian and military domains, there is probably still plenty for hackers to target.

There is no need – The Russians already own Ukraine: Much of Ukraine's infrastructure – notably the phone system – dates from the Soviet era. It is logical, therefore, that the Russians have already wired the phone system for interception and, it would hardly be in their interest to take it down.[9] This explanation does not explain anything the Ukrainian side has or has not done, nor does it explain the lack of attacks on other systems such as power, natural gas distribution or finance. However, it may help to understand a lack of attacks on telecommunications, given that a cyber attack could disrupt a lucrative cyber espionage operation by alerting defenders that their systems have been penetrated and forcing a system scrub. Such action may not only knock out existing implants but also make the reinsertion of malware more difficult. The effects of cyber attack tend to be short term, while stealthy cyber exploitation can persist for years. Therefore, for strategic purposes, attacks such as Denial-of-Service (DoS) can be counterproductive. Well-designed technologies like Skype, however, which have end-to-end encryption, could lessen the value of cyber espionage over time (but not by much, because encryption does not protect if computers on one or both ends of the conversation are compromised), and increase the likelihood of denial-of-service attacks.

Neither Russia nor Ukraine wants such an escalation: In theory, the Russo-Ukrainian conflict is not a war between two states, but an insurgency and count-

8 Kelly Jackson Higgins. 'Lebanon Believed behind Newly Uncovered Cyber Espionage Operation,' *Information Week,* 31 March 2015, http://www.darkreading.com/attacks-breaches/lebanon-believed-behind-newly-uncovered-cyber-espionage-operation/d/d-id/1319695.

9 Jeffrey Carr, quoted in Patrick Tucker. 'Why Ukraine Has Already Lost The Cyberwar, Too,' *Defence One*, 28 April 2014, http://www.defenseone.com/technology/2014/04/why-ukraine-has-already-lost-cyberwar-too/83350/.

er-insurgency campaign over territory in eastern Ukraine. According to the Russian Government, Russian forces are not even in the fight, and thus far, neither country's infrastructure (outside the battle zone) has been touched. In this context, if Russia were to attack Ukraine's infrastructure or vice versa it would be hard to ascribe the attack to separatists, who likely would not possess the requisite advanced hacker skills among their 'patriotic hacker' ranks. Organised crime syndicates may have the technical expertise, but may lack the trust or the intelligence-informed approach required. Still, given that both of these groups enjoy some state protection in Russia, such an operation is not out of the question. The more important point here is that any such escalation could change the narrative of the conflict from an inter-ethnic squabble to an interstate war. An obvious attack by Russia against Ukraine's infrastructure may conflict with its current political narrative. A Ukrainian attack against Russia could be a warning signal to Moscow that it will have to pay a price for its actions (a sporty move indeed), as well as a sign that it cannot do better in a conventional fight with the Russian military. A wild card here is that cyber war techniques in 2015 may be viewed in and of themselves as unduly escalatory, but this fear likely does not apply to cyber attacks precisely focused on enemy military targets in theatre where their use ought to seem no more alarming than the use of, say, electronic warfare. Finally, it is important to remember that two nuclear states may easily prefer fighting without resorting to nuclear weapons; in cyber warfare, many analysts have noted that any two sides are likely riddled with exploitable vulnerabilities.[10]

Cyber war is not a 'silver bullet'. Proponents of cyber war argue that attacks are cheap, asymmetric, effective, and risk-free. But what if they are wrong? A truly successful cyber attack – one that does more than simply annoy defenders – is harder than it looks. Penetrating systems without getting caught requires technical expertise that is in short supply. Preoperational reconnaissance and intelligence gathering of the kind required to create politically interesting effects such as against national critical infrastructure, or to target military defence systems takes a long time and may not produce practical results. In 2015, it is also possible that neither Russian nor Ukrainian systems are sufficiently wired to allow for easy access and manipulation. Human-in-the-loop safeguards, for example, may prevent truly serious damage from occurring except on rare occasions. Both crit-

A truly successful cyber attack – that does more than simply annoy defenders – is harder than it looks.

10 'The Russians and Ukrainians have some of the best computer people in the world, because of the Soviet legacy military industrial complex,' says Taras Kuzio, a Ukraine expert at the School of Advanced International Studies at Johns Hopkins University. 'These [Ukrainian] guys are fantastic. So if the Russians tried something like a cyberattack, they would get it right back. There would be some patriotic hackers in Ukraine saying, 'Just who are the Russians to do this to us?' from Mark Clayton. 'Where are the cyberattacks? Russia's curious forbearance in Ukraine,' *Christian Science Monitor*, 3 March 2014, http://www.csmonitor.com/World/Security-Watch/2014/0303/Where-are-the-cyberattacks-Russia-s-curious-forbearance-in-Ukraine.-video.

ical infrastructure and combat systems are designed to operate under a great deal of stress and unexpected events. Some states may already have calculated that the effects of cyber war are limited, temporary, and hard to repeat. Attackers also fear that digital weapons may work only once before defenders can plug the necessary holes. In this light, is developing a cyber war arsenal really worth it?

4 Conclusion

In 1972, when Chinese Premier Zhou Enlai was asked about the significance of the French Revolution of 1789, he famously said, 'It is too soon to say'.[11] With that logic in mind, it must be noted that the Internet is still a baby, and that cyber attacks are still in a nascent stage. Despite the prevailing 25 May 2015 ceasefire, the Russo-Ukrainian conflict is not over. Currently, it could be that neither side wants to escalate this somewhat localised conflict into the realm of interstate war, and this may inhibit operations otherwise warranted in less opaque circumstances. Both parties to the conflict are still exploring their best options, and both are surely upgrading their traditional and digital military arsenals. Finally, it is hard to say what current cyber operations may come to light in the future. However, in mid-2015, the preponderance of evidence suggests that the easy assumption that cyber attacks would unquestionably be used in modern warfare has come up wanting.

11 Alas, one of the greatest quotes in international relations of the 20th century may have been misunderstood, as Chou was actually referring to French protests of 1968. However, a diplomat present at the time said Chou's comment was 'too delicious to invite correction.' Dean Nicholas 'Zhou Enlai's Famous Saying Debunked,' *History Today*, 15 June 2011, http://www.history-today.com/blog/news-blog/dean-nicholas/zhou-enlais-famous-saying-debunked.