Strategic Defence in Cyberspace: Beyond Tools and Tactics

by
Richard Bejtlich

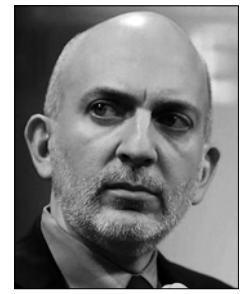
Chapter 18 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

In Chapter 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.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Strategic Defence in Cyberspace: Beyond Tools and Tactics



Richard Bejtlich
The Brookings Institution

1 Introduction

The digitisation of information, which began during the Second World War, has significantly deepened the relationship between human beings (from the individual to the nation-state) and unstructured data, structured information (such as a databases), and intelligence (information of political or military value). Every part of society has benefited from information technology; however, as we have increasingly become data-reliant, our adversaries have sought to leverage information against us. Attackers and defenders now battle for access to, and control of, information in the political, economic, military, and social spheres. In military parlance, data has become a virtual 'high ground' from which the better-informed can influence an adversary.

The Ukrainian Government currently finds itself at a tactical disadvantage *vis-à-vis* Russia, both on the traditional field of battle as well as in cyberspace. However, cyber security, especially at the national level, is a strategic game, and Kyiv can make smart investments that will pay off over the long run. In Ukraine, as in every other nation-state, practitioners, academics, policy-makers, and the public are individually and collectively vexed by the question of how to defend data, information, and intelligence. Part of the problem is that adversaries do not have one or even several attack strategies at their disposal: they can steal, destroy, deny access to, or even alter information – as well as the systems that store, process, and display it to its ostensible owners.

Digitised information is a human product which resides in mechanical devices built by engineers and programmers, and so decision-makers naturally turn to the technical community for answers to these challenges. Technical proposals take many forms. Several frequently appear in policy-making circles: we could scrap the internet entirely and replace it with a 'more secure' alternative;[1] we might build software that is 'not hackable,' possibly through 'leap ahead' technologies that make defence easier than offense (which is today manifestly not the case);[2] or we can outsource our security to third-party vendors.[3] These are all technical ideas, but they are generally not feasible for a variety of reasons. More fundamentally, it is dangerous to rely solely on technology to mitigate core security problems.

2 The Limitations of Technology-driven Approaches

Technology plays an important role in defending data. Thoughtfully designed networks, higher quality software, and agile start-ups can frustrate opportunistic intruders seeking easy prey. Unfortunately, well-resourced, professional attackers sometimes have long-standing missions to compromise specific high-value targets, whether for information theft or data manipulation. They will not give up until their mission requirements change or until they succeed in their assignment.

Digital defenders may only get a glimpse of the intruder, and often this comes far too late in the game. Whereas the victim's perspective is usually narrow and incomplete, professional attackers are persistent and know exactly what they are targeting. According to the Mandiant 2015 *M-Trends* report, the median number of days in 2014 that a successful threat group was present on a victim's network before detection, was 205. In one case, an adversary had maintained unauthorised access for over 8 years.[4] Even after discovery, organisations can spend months trying to remove the intruder. In February 2015, the *Wall Street Journal* reported that the US State Department continued to be plagued by foreign hackers fully three months after the agency confirmed reports of an intrusion.[5]

> *A technology-centric worldview obsesses about a static, one-time exchange between attacker and defender.*

This relationship between security and time is central to protecting digital

1 Thom Shanker. 'Cyberwar Chief Calls for Secure Computer Network,' *New York Times*, 23 September 2010, http://www.nytimes.com/2010/09/24/us/24cyber.html; John Markoff. 'Do We Need a New Internet?' *New York Times,* 14 February 2009, http://www.nytimes.com/2009/02/15/weekinreview/15markoff.html.

2 Jim Garamone. 'DARPA Director Discusses Cyber Security Challenges,' *DoD News,* 1 October 2014, http://www.defense.gov/news/newsarticle.aspx?id=123307.

3 Over 400 vendors demonstrated their products and services at the RSA Conference in San Francisco, California in April 2015. RSA Conference 2015 vendors, http://www.rsaconference.com/events/us15/expo-sponsors.

4 The median number for 2013 was 229 days. FireEye, *M-Trends 2015: A View from the Front Lines* (Milpitas, CA: FireEye Corporation 2015), https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf.

5 Danny Yadron. 'Three Months Later, State Department Hasn't Rooted Out Hackers,' *Wall Street Journal*, 19 February 2015, http://www.wsj.com/articles/three-months-later-state-department-hasnt-rooted-out-hackers-1424391453.

resources. An analysis of time intervals is key to understanding the interaction between attackers and defenders, but in general the security community does not sufficiently understand or appreciate the nature and consequences of this relationship. A technology-centric worldview obsesses about a static, one-time exchange between attacker and defender. This is not an accurate description of the real world, which is populated, not with mindless code, but with rational and irrational human beings who are both intelligent and adaptive adversaries and who observe their targets, allocate resources, and make dynamic decisions in order to accomplish their goals.[6]

Digital defenders ignore these facts at their peril. The interactive and time-dependent nature of network attack and defence leads to the promotion of suboptimal approaches to security. The emphasis on 'cyber hygiene' is illustrative.[7] To defeat intruders, this method promotes knowing one's network, removing unauthorised systems, patching vulnerabilities, and improving configurations. All of these are certainly both requisite and commendable defensive steps. However, they are insufficient when confronting an attacker who has the time and resources to adapt to and overcome the target's defences. 'Washing cyber hands' is helpful when minimising the spread of mindless germs, but it is less effective when those germs are as smart as, or better-resourced and motivated than, the hand-washer.

3 Strategic Thought in Cyber Defence

To better address the dynamic challenge of continuous interaction between adaptive, intelligent adversaries, this chapter advocates the application of strategic military concepts to conflict in cyberspace. Armed conflict has long been characterised as a struggle between persistent adversaries over time. However, the advent of mass armies, modern weapons, and nation-state warfare in the late 18th and early 19th centuries took this concept to a higher level. During the 20th century, military strategists therefore had to think beyond the traditional dichotomy of strategy versus tactics. Over time, they codified multiple 'levels of warfare'.

Beginning in the 1980s, U.S. Army doctrine described three levels of war: strategic, operational, and tactical.[8] These built on previous writings and lessons learned, from Napoleonic battles to Soviet military planning. National goals and policy – sitting above the strategic level of war – were incorporated into doctrine, although this can be confusing given that the word 'strategic' often appeared in both the model's name and one of its primary elements.

6 John R. Boyd. 'The Essence of Winning and Losing,' unpublished PowerPoint presentation, 1985, http://www.danford.net/boyd/essence.htm.

7 Jonathan Trull. 'Practice Makes Perfect: Making Cyber Hygiene Part of Your Security Program,' *CSO Magazine*, 3 March 2014, http://www.csoonline.com/article/2891689/security0/practice-makes-perfect-making-cyber-hygiene-part-of-your-security-program.html.

8 United States Department of the Army, *Field Manual 100-5: Operations* (Washington, DC: US Army 1982), http://cgsc.contentdm.oclc.org/cdm/compoundobject/collection/p4013coll9/id/48/rec/10.

Policies and Goals

|

Strategies

|

Operations (including Campaigns)

|

Tactics

|

Tools

Figure 1-1 – Strategic Thought, Adapted for Digital Conflict

In this chapter, the author argues that decision-makers need to better understand the role of technology in strategic thought, and so it adds a new level below the tactical layer: 'tools'. Certainly in physical warfare one uses 'tools' to inflict kinetic damage. In the digital world, the model explicitly introduces tools in order to show practitioners where they fit in strategic thinking. Too many digital security professionals believe tools are the sole focus of defensive action. By placing tools at the bottom of the model, they appear, in the author's opinion, in their proper place. Furthermore, in this model, the term 'campaign' is included at the operational level. 'Campaigns' and 'operations' are sometimes interchanged, so both appear to reduce confusion.

Too many digital security professionals believe tools are the sole focus of defensive action.

These five levels are depicted in Figure 1-1. Policies and goals are broad statements by organisational leadership that describe the desired purpose of the strategic programme. Strategies are concepts for employing organisational resources to accomplish the stated policies and goals. Operations (which in this schema are organised into campaigns) are sets of activities designed to implement strategies that are pursued over days, weeks, months, or even years. Tactics are actions taken within individual encounters with an adversary, and serve as the atomic elements of a campaign. Tools are the digital equipment with which an actor implements tactics.

All of these elements must be connected in order to achieve successful outcomes. Before explaining how these five levels can improve digital defence, it is important to recognise that I am not advocating the 'militarisation' of cyberspace – which is a valid concern of many analysts. For example, in 2013, Jason Healey wrote in *Foreign Affairs* that the military had 'prioritised one national security goal – more spying and attack capabilities – above all others'.[9] A *Forbes* journalist defined the problem as 'giv[ing] a military character to' it, 'equip[ping] [it] with military forces and defences' or 'adapt[ing] [it] for military use',[10] This author, while generally disagreeing with these premises, does not equate strategic thought with militarisation. The purpose of this chapter on strategic thought is to familiarise defenders with another strategy to protect information, one suited to the timescales and interactive nature of modern computer intrusions.

4 Traditional Security within the Strategic Model

Squaring traditional security concepts with the strategic model contributes to a rich discussion of digital defence. Typically, network defenders concentrate on tools and tactics, which are in turn dominated by the notions of security software, software security, and securing software. Security software consists of programs written by vendors, open source developers, and individual security teams that are designed to detect, frustrate, and remove adversaries. Software security refers to the process of writing computer programs that are free from coding, process, and logic flaws, optimally using a process such as the Building Security In Maturity Model (BSIMM).[11] Securing software is a process to enable the 'cyber hygiene' model, whereby defenders take various tactical steps to reduce the likelihood of compromise.

Beyond the security team, one finds multiple layers of management, including a chief security or information security officer (CSO or CISO), one or more chief technology or information officers (CTO or CIO), other members of the so-called 'C-suite' including the chief financial or operating officers (CFO, COO), and ultimately the chief executive officer (CEO) and board of directors. At the nation-state level, some governments have appointed cyber security coordinators reporting to the head of government. Recent examples include the United States, the United Kingdom, Germany, Russia, Japan, and France.[12] In China, President Xi Jinping personally leads the country's top information security group.[13] One would think

9 Jason Healey. 'How Emperor Alexander Militarized American Cyberspace,' *Foreign Policy*, 6 November 2013, http://foreignpolicy.com/2013/11/06/how-emperor-alexander-militarized-american-cyberspace/.

10 Sean Lawson. 'Is the United States Militarizing Cyberspace?' *Forbes*, 2 November 2012, http://www.forbes.com/sites/seanlawson/2012/11/02/is-the-united-states-militarizing-cyberspace/.

11 BSIMM, https://www.bsimm.com/.

12 French Ministry of Foreign Affairs and International Development, 'France and cyber security,' http://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/.

13 Shannon Tiezzi. 'Xi Jinping Leads China's New Internet Security Group,' *The Diplomat*, 28 February 2014, http://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/.

that, with so much focus on cyber and information security at the upper levels of management, defence strategies would be clear. However, despite numerous recent high-profile breaches, security leaders continue to fret that their 'organisation's business leadership didn't provide them the support and space they need to secure their organisations properly'.[14]

Improving the dynamics of strategic thought according to the proven military model can help organisations and nation states move beyond a 'tools and tactics' focused approach. The latter is by far the prevailing paradigm. For example, one 2014 RSA Conference presentation encouraged attendees to 'exploit pet projects' and 'capitalise on timely events' by using the 'near-death experiences of others to justify security spend'.[15] One 2015 article written for security managers stressed the need for more capable software, stating that 'a CISO must successfully address many challenging elements when procuring a new security technology solution'.[16] In 2014, Symantec's Senior Vice President for Information Security said that only 45% of cyber attacks are prevented by anti-virus software, calling it a 'dead' technology.[17] Writing secure software, while a laudable goal, continues to be difficult, even for leading companies like Microsoft. Bill Gates accelerated the programme to find a secure development lifecycle in 2002, but the vendor continues to release patches for 'remote code execution' vulnerabilities in core Microsoft platforms on a monthly basis. In brief, we need more than tools and tactics to counter digital adversaries.

When trying to learn how to communicate with higher level managers and CISOs, agency leads, and policy-makers are bombarded with advice like the following:

> *'One of the most strategic skills a security chief can bring is the proficiency in translating security speak into the language of business risks and financial ROI [return on investment] terms... At the board level, the ability to show dollar return on security initiatives is critical to ensure continued executive support on security investments'*.[18]

The problem with the focus on tools and tactics, and related topics of risk and ROI is that higher-level management and boards do not feel connected to the true defensive posture of their organisation. Because leaders have not been valued parts of the security program development process, they think security is mainly an issue to be solved by technical professionals. Their experience with the IT and security

14 George V. Hulme. 'The CSO's failure to lead,' *CSO Magazine*, 9 June 2014, http://www.csoonline.com/article/2360984/security-leadership/the-cso-s-failure-to-lead.html.

15 John B. Dickson. 'Getting Your Security Budget Approved without FUD,' RSA Conference 2014, http://www.rsaconference.com/writable/presentations/file_upload/ciso-w04a-getting-your-security-budget-approved-without-fud.pdf.

16 Craig Shumard. 'CISOs Face Tough Challenges When Procuring Security Technologies,' Tenable Network Security, 5 March 2015, http://www.tenable.com/blog/cisos-face-tough-challenges-when-procuring-security-technologies.

17 Danny Yadron. 'Symantec Develops New Attack on Cyberhacking,' *Wall Street Journal*, 4 May 2014, http://www.wsj.com/articles/SB10001424052702303417104579542140235850578.

18 Danelle Au. 'Getting the CISO a Seat,' *Security Week*, 16 July 2012, http://www.securityweek.com/getting-ciso-seat.

worlds has led them to approach security as an issue of approving budgets to purchase ever-more-costly security software. The *Christian Science Monitor* reported the following in February 2015:

> *'In a survey commissioned by defence contractor Raytheon of 1,006 chief information officers, chief information security officers, and other technology executives, 78 percent said their boards had not been briefed even once on their organisation's cybersecurity strategy over the past 12 months ... The findings are similar to those reported by Pricewaterhouse-Coopers in its Global State of Information Security Survey last year in which fewer that 42 percent of respondents said their board actively participates in overall security strategy'.*[19]

In light of these challenges, this chapter advocates making boards and higher-level managers integral aspects of the security process, by way of strategic thought.

This chapter advocates making boards and higher-level managers integral aspects of the security process.

5 Cyber Security without Strategy

The following scenario will help the reader understand how the application of strategic cyber security principles can better protect digital assets. A private organisation suffers targeted attacks by both criminal and nation-state threat groups, which not only compromise the organisation but also steal intellectual property including trade secrets, sensitive commercial data, and other digital resources.

The traditional 'tools-and-tactics' security model is characterised by suboptimal communication and poor alignment between the management, board, and security team. The latter, led by the CISO, is determined to counter the adversary. Their first instinct will be to take some concrete action: to hire new personnel, to develop a new capability, to adopt a new tactic, or to purchase a new software tool. Next, they will attempt to translate their plan into 'business speak', and the CISO will develop an argument based on an ROI estimate that includes the cost of the initiative, the amount of money it should save (if all goes well), and a mathematical calculation of the overall risk to the enterprise.

If asked by the CEO or board to explain his or her rationale, the CISO will reply that a tools-and-tactics approach will save the enterprise money and reduce its level of risk. Finally, the management will give the proposal a green light, or send the CISO back to the drawing board.

19 Jaikumar Vijayan. 'After high-profile hacks, many companies still nonchalant about cybersecurity,' *Christian Science Monitor,* 19 February 2015, http://www.csmonitor.com/World/Passcode/2015/0219/After-high-profile-hacks-many-companies-still-nonchalant-about-cybersecurity.

This budget request cycle is repeated *ad nauseam*, until management gets wise to the fact that network security ROI seems to have an Alice-in-Wonderland quality about it: the more money they spend, the more money they are supposed to save. Eventually, management realises that security is a lot more about loss prevention than revenue generation, and they begin to feel disconnected (and disaffected) from the defence of their digital resources. Further, they recognise that their organisation is one of many whose boards are not briefed on real strategy, and who have in fact never participated in serious strategy formulation.

6 Strategic Cyber Security

A strategic cyber security programme, by contrast, does not begin with tools and tactics, but with an articulation of one or more programme goals. First, the strategy-minded CISO gets executive buy-in to those goals. To that end, the CISO must incorporate all levels of strategic thought, starting with the board and CEO – everyone must feel ownership and participation. The smart CISO recognises that security is a journey, not a destination, and that relationship building requires an ability to translate between technical and non-technical vocabularies.

The CISO ensures that the programme goals accurately govern the objectives of the enterprise's digital security programme. In our scenario, the CISO, board, and CEO all agree that, with respect to intellectual property, trade secrets, and sensitive data, the new policy goal is to minimise loss due to intrusion. This statement implies that everyone understands that stopping all adversaries and all attacks is simply not possible, especially when dealing with nation-state actors and some advanced criminal groups.

The primary objective of this exercise is to achieve consensus on a simply stated, non-technical programme goal. No in-depth technical discussion is needed to achieve consensus, although the CISO must ensure that all goals, policies, and strategies are technically feasible. With a mandate in hand, the CISO can confidently work with his or her security team to plan the necessary operations and campaigns and, if necessary, acquire new tools and tactics to facilitate them. Together, they decide to implement a network security monitoring (NSM) operation, defined as the collection and escalation of indications and warnings to detect and respond to intruders.[20] The security team begins the long-term, strategic process of hunting for hostile cyber attack campaigns, encompassing both known and unknown intrusion patterns.

> *The primary objective is to achieve consensus on a simply stated, non-technical programme goal.*

20 Richard Bejtlich. *The Practice of Network Security Monitoring* (San Francisco, CA: No Starch 2013).

The CISO, board, and CEO all agree that a second programme goal is the rapid detection, response, and containment of cyber threats. This goal helps to ensure that when intruders breach the perimeter defences, the game is far from over. Defenders can still win, so long as they contain the threat before the attacker can accomplish his or her ultimate mission. Therefore, the security team will develop strategies to identify compromises quickly, determine their nature, give them some level of attribution, and above all develop a plan to stop the attacker from accomplishing his or her mission.

At the tactical level of individual engagements with the adversary – the equivalent of battles in war – the security team will have myriad decisions to make, including whether to dislodge the intruder immediately or whether to watch the intruder for a time in order to collect valuable intelligence. Some tactics govern how specific tools or techniques can be used, such as when Star Trek personnel switch their hand phasers between 'stun' and 'kill'. As always, the adversary gets a say in what happens, but from the enterprise's point of view, programme goals, policies, and guidelines should be written to govern this entire process.

7 The Relevance of Campaigns

Central to the concept, and success, of a strategic security program is the campaign, which functions at the operational level. In some sense, the maturity of a security programme can be derived from the attention shown by the CISO and his or her security team to campaign development, and the understanding of campaign progress and analysis by top management. Consider the following quote from a February 2015 Reuters report on defence contractor Lockheed Martin:

> *'[Chief Executive Officer Marillyn] Hewson told the company's annual media day that Lockheed had faced 50 'coordinated, sophisticated campaign' attacks by hackers in 2014 alone, and she expected those threats to continue growing'.*[21]

When Ms. Hewson spoke in terms of campaigns, she showed that her security team thinks and works at an advanced level. It is likely that Lockheed also aligns campaigns with specific threat actors and motives. Speaking about specific campaigns and ranking them in terms of sophistication and impact permits a vastly more meaningful discussion with other executives, the board, and other stakeholders. The CEO should be able to speak in detail about the threat actors behind the campaigns, including their means and motives, as well as illustrative examples of each campaign and how the security team detected and responded to them. The term 'campaign' also matches well with non-technology business operations such as marketing campaigns and sales campaigns.

21 Andrea Shalal. 'Lockheed sees double-digit growth in cyber business,' *Reuters*, 18 February 2015, http://www.reuters.com/article/2015/02/19/us-lockheed-cybersecurity-idUSKBN0LN03K20150219.

Contrast this approach with a recent briefing by Japan's National Institute of Information and Communications Technology, which appeared in the *Japan Times*:

> *'The number of computer attacks on government and other organisations detected in Japan doubled in 2014 from the previous year to a record 25.66 billion, a government agency said Tuesday'.*[22]

Discussing individual attacks has limited value, as discrete incidents include everything from a suspicious TCP packet, to an odd computer port, dubious SQL query, or 'phishy' email. On the other hand, how can anyone devise a credible programme goal to counter over 25 billion attacks? The sweet spot lies in the middle, in grouping the primary threats and threat actors into coherent and logical campaigns. This is the best way for the enterprise – or a nation state – to counter an interactive and adaptive adversary.

8 Strategic Cyber Defence in Ukraine

The government of Ukraine, which has tense relations with Russia and is embroiled in an ongoing war, is likely the target for many ongoing cyber attack campaigns. This author advises that the only way to counter an offensive campaign is with an equally determined defensive campaign.

> *The only way to counter an offensive campaign is with an equally determined defensive campaign.*

In April 2015, the security company Looking Glass exposed 'Operation Armageddon,' which it described as a cyber espionage campaign (active since 2013) designed to provide a 'military advantage' to Russia by targeting Ukrainian government, law enforcement, and military officials for information of intelligence value. The researchers found a 'direct correlation' between digital attacks and the ongoing war, including an 'alarming' blend of cyber espionage, physical warfare, and geopolitics.[23] Recent reports by security companies Trend Micro and FireEye describe other Russian campaigns, assigned the monikers 'Operation Pawn Storm' and 'APT28', respectively.[24] According to FireEye, APT28 appeared to target individuals affiliated with European security organisations, including the North Atlantic Treaty Organisation (NATO) and the Organisation for Secu-

22 'Cyberattacks detected in Japan doubled to 25.7 billion in 2014,' *Japan Times*, 17 February 2015, http://www.japantimes.co.jp/news/2015/02/17/national/crime-legal/cyberattacks-detected-in-japan-doubled-to-25-7-billion-in-2014/.

23 Looking Glass Security, *Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare* (Bumpas, VA: Looking Glass Security Corporation 2015) https://lgscout.com/wp-content/uploads/2015/04/Operation_Armageddon_FINAL.pdf.

24 Loucif Kharouni, et al, *Operation Pawn Storm: Using Decoys to Evade Detection* (Trend Micro Incorporated: Irving, TX 2015) http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf and APT28 https://www.fireeye.com/resources/pdfs/apt28.pdf.

rity and Cooperation in Europe (OSCE) which the Russian Government has long cited as existential threats.[25]

Similarly, Russian non-government groups such as CyberBerkut have been active against NATO and Ukrainian targets.[26] In March 2014, the group directed Distributed Denial of Service (DDoS) attacks against NATO's main website, the CCD COE website, and NATO's Parliamentary Assembly website.[27] In October 2014, on the eve of parliamentary elections in Ukraine, the website of the country's Central Election Commission suffered DDoS attacks.[28] The group has apparently also targeted US military contractors working in Ukraine, stealing and publishing documents about the movement of Western military equipment to Ukraine.[29]

Nation state security requirements are strategic in nature, and they do not frequently change. For what is seen to be a valid national security concern, states will devote enormous human and technological resources to achieve their objectives, and use a variety of methods and attack vectors. Neither does a state give up after one or even a hundred unsuccessful tactical engagements. Rather, it will adapt, and usually overcome defences eventually. The key factor that sets nation states apart from individuals and even hacker groups like Anonymous is *persistence*, and the ability to maintain persistence indefinitely.

Actors such as Russia also qualify as highly 'advanced'. Here is the author's working definition, published in 2009:

> *'Advanced means the adversary can operate in the full spectrum of computer intrusion. They can use the most pedestrian publicly available exploit against a well-known vulnerability, or they can elevate their game to research new vulnerabilities and develop custom exploits, depending on the target's posture'.*[30]

Recognising that any nation-state – in this case Russia – has the capability to adapt and overcome is one reason why threat attribution is so important, at all levels of strategic thought.[31] This means that any time the security team recognises a failed intrusion attempt as coming from an advanced persistent threat actor, they can be sure the foe will return with a new technique and perhaps even a new campaign.

25 *Ibid*.
26 'Berkut' is Ukrainian for 'special police force,' although CyberBerkut is a pro-Russian group.
27 'Ukrainian CyberBerkut takes down NATO websites,' *RT,* 16 March 2014, http://www.rt.com/news/nato-websites-ddos-ukraine-146/.
28 Vitaly Shevchenko. 'Ukraine conflict: Hackers take sides in virtual war,' *BBC News*, 20 December 2014, http://www.bbc.com/news/world-europe-30453069.
29 Jack Smith IV, 'Pro-Russian Hackers Expose U.S. Military Contractor Activity in Ukraine,' *Observer,* 2 March 2015, http://observer.com/2015/03/pro-russian-hackers-expose-u-s-military-contractor-activity-in-ukraine/.
30 Richard Bejtlich. 'What APT Is', *Information Security Magazine,* July 2010, http://www.academia.edu/6842130/What_APT_Is.
31 Richard Bejtlich. 'Five Reasons Attribution Matters,' *TaoSecurity Blog,* 30 December 2014, http://taosecurity.blogspot.com/2014/12/five-reasons-attribution-matters.html.

9 Conclusion

The Ukrainian Government currently finds itself at a tactical disadvantage vis-à-vis Russia, both on the traditional field of battle and in cyberspace. However, cyber security, especially at the national level, is a strategic game, and Kyiv can make smart investments that will pay off over the long run.

> *Cyber security, especially at the national level, is a strategic game.*

This chapter has argued for the need to apply strategic thought to digital defence. It began by advocating the utility of a military model in cyberspace, albeit without any desire for the militarisation of cyberspace. The author explained how the military mind set, based on conflict with dynamic, adaptive adversaries, is a more reliable strategy than the popular 'cyber hygiene' model. It then described the five levels of strategic thought, which link goals with policy, strategy, campaigns and operations, tactics, and tools. The author applied each level of strategic thought to a hypothetical network defence scenario. By integrating strategic thought into digital defence, this chapter demonstrated an alternative to technology-centric approaches that are not sufficient to defeat the adversary.

In a time of war, Ukraine is a natural target for many cyber threat actors and campaigns. The only way to counter them is to develop an equally determined defensive posture in cyber space.