2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

Winning and Losing in Cyberspace

Jason Healey
Saltzman Institute of War and Peace Studies
Columbia University SIPA
New York, NY, USA
jh3639@columbmbia.edu

Abstract: This paper examines cyber conflict using a lens of 'winning' or 'losing', or alternatively the role of 'victory' or 'triumph' compared to that of 'defeat', to draw broader conclusions about the dynamics of cyber power. To do so, the paper analyses writing on the general topic of winning over the years, then dives into the two most critical key case studies: the 2007 attacks on Estonia, and the 2008-2015 conflict between the United States and Iran. It addresses the most relevant factors for these cases, including a summary of the participants in the conflict and which side 'won' or 'lost' and why. After these case studies, the paper will address larger questions of winning and losing and the implications for our understanding of cyber power.

One of the factors that most distinguishes this research from previous work on cyber power is that winning is defined not only by actions on the network, but in terms of longer-term national security outcomes. For example, Estonia certainly lost tactically in 2007, as it was offline because of the Russian-encouraged denial-of-service attack. Regretfully, most analyses of the conflict do not explore any further, which is unfortunate, as while the Estonians lost the battle, they won the war. The Estonians refused to be coerced and are now renowned for their cyber security excellence, while NATO was warned of the dangers of cyber conflict, even building a new NATO cyber centre of excellence in Tallinn. Russia was thereafter known as a cyber bully. When expressed in terms of longer-term national security outcomes, it is clear they won both operationally and strategically.

Because this larger, non-technical view is often ignored in analyses of cyber conflict, this paper makes the case that the United States and nations that follow its model misunderstand the dynamics of cyber power and cyber conflict. Too much emphasis is placed on the success or failure of offensive and defensive capabilities, rather than on better or worse long-term national security outcomes.

The paper concludes with a short view of what winning might mean in more strategic national

security terms, and recommendations for the mechanics of national security policy-making.

Keywords: *cyber conflict, cyber power, case study, Estonia, Iran, winning, defeat, losing, victory*

1. INTRODUCTION

There is a deep misunderstanding of what constitutes victory in cyber conflict. In most writing on cyber power, what constitutes 'winning' or 'losing' is rarely ever specified. When winning is even discussed, it is most often applied to actions on the network, whether a target is taken down or intruded into; the basic units of analysis are computer systems or malicious ones and zeroes. Because cyber conflict is seen as such a technical area, this tactical and technical view has been the dominant view for decades, perhaps ever since 1991 when the idea of a 'digital Pearl Harbor' first took root.

However, this view gives far too much attention to actions on the network and not enough to actual national security outcomes. This is most apparent in the Estonian cyber conflict of 2007, widely seen in the US military as a defeat in which Estonia was 'wiped off the net,' but which was in fact a fairly crushing operational and strategic win for the Estonians.

Since cyber power is becoming far too important for such a fundamental misunderstanding, where a victory is mistaken for a defeat, this paper analyses past writing on the topic, distinguishing efforts which focus on the tactical or technical level from those at the strategic level. The paper examines the two most illustrative case studies: Russian patriotic hackers against Estonia in 2007, and the long back-and-forth campaigns between the United States / Israel and Iran.

Defining victory in cyberspace, the next section argues, has been difficult for several reasons, including those mentioned above. However winning itself ought to be described as like any other kind of national security endeavour; that is, leading to better national security outcomes. Those outcomes might, in cyberspace, come from maximising hard power (espionage and attack capabilities), soft power (alliances, private-sector partnerships, influence), or economic power (trusted cyber companies, and a strong Internet-enabled economy). The paper then concludes with recommendations for policy-makers.

2. PAST WRITING ON WINNING AND LOSING

Winning is like 'power', in that it is 'surprisingly elusive and difficult to measure. But such problems do not make a concept meaningless.' (Nye, 2010). Yet to date, very little writing on winning or losing in cyber conflicts has been particularly specific about just what either might mean. There has been a strong tendency, especially in news articles or opinion pieces, to insist that the 'other guys' (often China, at least in the United States) are winning and 'our side' is

doomed to lose until the writer's recommendations are implemented. The most useful literature (including some with these weaknesses) falls into two relatively neat categories: the tactical and technical or operational levels, and the broader strategic or national security.

A. Winning and losing at the technical and tactical or operational level

The first set of useful literature focuses particularly on 'getting hacked' (if thought of as a technical issue) or on particular engagements or strings of engagements as part of a campaign (if thought of, in military terms, as the tactical and operational levels of war). Many pieces in this type imply that winning means keeping at bay criminal hackers, such as a recent corporate report on *Winning the Cyber War*. This report, published by Deloitte in cooperation with Symantec, recommends 'a clearer understanding of the risks posed to them and the level of protection needed to combat these threats, in order to inform an effective data protection strategy' (Deloitte, 2015).

More serious debate on war as it is meant in national security terms centres on winning as a successful use of cyber capabilities in a national security-related engagement or campaign.

The best example here is not of winning, but of losing, and not just any cyber battle, but a 'digital Pearl Harbor', where '[a]n aggressor nation could ... derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals', as then-Defense Secretary Leon Panetta expressed it in late 2012 (Bumiller and Shanker, 2012). While the concept of an 'electronic Pearl Harbor' has been around (and much derided) since 1991, it does have an implied meaning of victory and defeat: the attacker succeeds in a devastating first strike against military or civilian targets.[1]

The attacker wins if their capabilities work as expected and take down their targets; in the zero-sum world of employment of cyber capabilities, the defenders have lost. This use of 'winning' appears to be precisely what Panetta had in mind, as immediately after his speech discussing a digital Pearl Harbor:

> 'Defense officials insisted that Mr. Panetta's words were not hyperbole, and that he was responding to a recent wave of cyberattacks on large American financial institutions [later blamed on Iran]. He also cited an attack in August on the state oil company Saudi Aramco, which infected and made useless more than 30,000 computers' (Bumiller and Shanker, 2012).

General Keith Alexander (former Director of the National Security Agency and Commander of US Cyber Command) highlighted the military view of winning engagements, saying that 'leaders want to dominate cyber-space in any encounters with adversaries' (Alexander, 2014). Most US military services have organisations committed to 'information dominance', such as the Army Information Dominance Centre and the Navy Information Dominance Corps. The top Air Force information officer also wears the hat of 'Chief of Information Dominance'.

It is probably this view that led Alexander, and his successor Admiral Michael Rogers, to see the attack on Sony Motion Pictures as a win for North Korea. The attacks destroyed data and

1 The first known use was by Winn Schwartau in congressional testimony on 27 June 1991.

cost perhaps hundreds of millions to clean up. Alexander later emphasised that 'destructive attacks that destroy data permanently, whether it hits Sony, a power [grid], a government, financial institution, the destruction of data in cyberspace is bad', and by implication a defeat as well (Gonzalez, 2014).

In the same vein, the hacker collective Anonymous has been said to be winning the war on Islamic State because it is taking down websites or social media accounts (Roberts, 2015), and the number of websites taken down has been a tally for success in cyber conflicts from Israel-Palestine in 2000 (Gambill, 2000), to India-Pakistan in 2000 (Nanjappa, 2010) and 2015 (Singh, 2015).

There are also classic examples from the US and Israeli cyber conflict with Iran as well as the 2007 attacks on Estonia, which will be examined in more depth below.

B. Winning and losing at the strategic level

The second set of useful literature looks at winning at the strategic level (the analysis of national power, far grander than tactics or operations), which is not the same as succeeding with a strategic attack (such as massive bombing to weaken an enemy's morale or ability to wage war). Winning at the tactical, technical, or operational levels means keeping out hackers or successful engagements; winning at the strategic level has far more at stake: strategic political objectives, broad national advantage or military defeat.

A first key theme is that defeat in a cyber battle might be defined best by the impact on a traditional military fight; for example, that successful intrusions give 'China the potential capability to delay or disrupt U.S. forces without physically engaging them – and in ways it lacks the capability to do conventionally' (US China Commission, 2008).

China is often portrayed as the victor in cyber espionage against the United States (and other countries). China is seen as winning because repeatedly successful campaigns over time are seen as giving it the upper hand in national security competition, even dominance costing billions of dollars in annual harm (US China Commission, 2015; IP Theft Commission, 2013). Even more starkly, Russia is believed not to have had to unleash a 'conventional' cyber conflict of denial of service attacks in the Estonia 2007 model because it already had such cyber dominance that such attacks would be counterproductive (Tucker, 2014). And even before the Snowden revelations, a common theme in my conversations with Chinese government officials was that everywhere they looked they saw the United States on the commanding heights of cyberspace.

Kuehl and Miller (2009) helpfully examined how losing at the tactical level could force a loss at the strategic level. America tends to lose such first battles, but then rally and win the follow-on war. But perhaps US dependence on cyber infrastructure would lead to a different result if America lost the first cyber battle in a digital Pearl Harbor? They refer to perhaps the classic definition of winning, but one that shows up surprisingly rarely in the cyber literature: '[w]inning that future war – defined in Clausewitzian terms as the attainment of strategic political objectives – thus may depend on successfully waging and winning the 'first battle in cyberspace'.

The Stuxnet attack against Iranian nuclear enrichment capability is one of the few occasions where the cyber discussion has focused on winning as achieving strategic political objectives. This attack disabled up to 1,000 Iranian centrifuges (Sanger, 2012), but did this meet the objectives? If the goal was to stop the programme, then it was a failure, as it did not succeed in stopping Iran or denting the regime's determination to develop a nuclear weapons capability (Rid, 2013; Barzashka, 2013; Lindsay, 2013). However, if the goal was to impose even a slight delay and keep the Israelis from launching pre-emptive air strikes, then perhaps the White House can feel that it won. This view aligns with definitions of cyber power such as 'the ability to use cyberspace to create advantages and influence events in other environments and across the instruments of power' (Kuehl, 2009).

One reason why successfully meeting political objectives seems to be such a scarce metric for winning is that it is hard to find any evidence of any strategically successful cyber attacks (Healey, 2013; Valeriano & Maness, 2015; Gartzke, 2013). According to Rid, 'the political instrumentality of cyber attacks has been starkly limited and is likely to remain starkly limited'.

Indeed, even when 'winning' might seem straightforward, as in the case of Chinese espionage, the analysis is almost entirely about what the United States has lost, not how the stolen intellectual property has enriched China. The United States may indeed be having hundreds of billions of dollars' worth of intellectual property stolen, but how much of that gain is China actually capturing, and is it enough to meet Chinese political objectives, given the price they have paid in worsening relations with nations from whom it has stolen?

3. CASE STUDIES OF MAJOR CYBER CONFLICTS

Many of the specific case studies of cyber conflict remain classified by national intelligence services or hidden by corporations not willing to release data for fear of embarrassment or because of its commercial value. Accordingly, researchers are forced to use a relatively limited set of cases from which to draw conclusions. Fortunately, two of these, Estonia and the conflict between Iran and the United States and Israel, are both illustrative and important case studies. There is a wealth of public information, and both have been discussed frequently by key policy-makers.

A. Estonia, 2007

The 2007 campaign of cyber attacks against Estonia by Russian patriotic hackers, ignored or even encouraged by the Kremlin, is by far the most instructive. In the context of rising Estonian identity to the perceived detriment to Russian interests, the proximate cause of the campaign was the Estonian government choosing to move the Bronze Soldier, a statue of a Red Army soldier, along with the bodies of several unknown soldiers from World War Two. The relocation, from the centre of Tallinn to a military cemetery, led to a couple of nights of rioting in the city by Russian-speaking Estonians, and a campaign of denial of service attacks in several waves over the next few weeks, peaking on 9 May, the anniversary of the defeat of Nazi Germany (Schmidt, 2013). It was a classic cyber conflict, but not a cyber war; no one died from the cyber attack, and it caused only transient harm to disabled government, financial and other websites.

The immediate goals of the attacks appear to be straightforward; to use cyber capabilities as a 'cyber riot' or protest, to express displeasure over the move and to coerce the government to cancel it. This was a common message of the Russian-language media at the time. In the broader context, the goal was probably to help flex Russian power in the perceived 'near abroad' state of Estonia, once part of the mighty Soviet Union but now part of NATO. By ignoring or encouraging cyber attacks by Russian patriotic hackers, including condemnation by Russian President Vladimir Putin against those who 'desecrate memorials to war heroes' (BBC News, 2007), Moscow could send a message without seeming to be directly involved (Healey, 2013).

Most analyses of the campaign pivot around the theme that the Russian attack was so successful that Estonia 'more or less cut itself off from the internet' (Economist, 2010), as I have had General Alexander tell me (Alexander, 2013). Other Pentagon cyber officials were even more pointed: 'Why are the Estonians considered cyber experts? All they did is get knocked off the net'. Many Estonian websites were indeed knocked offline, and the Russian patriotic hackers were flooding Estonian networks with so much traffic that the Estonians were forced to disconnect themselves from international traffic at their local Internet Exchange Point (Schmidt, 2013). But, unfortunately, this analysis of the tactical and technical truths of the campaign is also beside the larger point. The conflict might have been a tactical defeat for the Estonians, but it was a clear operational win. Even after several weeks of disruptive attacks, the Estonians still moved the statue. That is, they refused to be coerced by the Russian exercise in cyber power. One of the smallest nations on the planet, with just 1.3 million people, no tanks, and no fighter aircraft, stood up to one of the most powerful.

Indeed, if the Kremlin's larger goal in ignoring and encouraging the attacks was to flex Russian power and keep Estonia cowed, then the campaign was a strategic loss for Russia as well. The Kremlin, after the campaign of attacks, emerged with its power somewhat diminished. NATO considered the Russian cyber attack on a member as a 'wake-up call' for the alliance, leading to response plans, wargames, and the creation of a new cyber centre of excellence – in Tallinn, Estonia (Healey and Jordan, 2014). The Estonians, in part because of the 2007 attacks, were feted in Washington and European capitals and are 'renowned for cyber security' (Economist, 2012).

The Estonians did not lose in 2007; in fact it wasn't even close. This means that the US military, the military force that has most embraced cyber capabilities, cannot distinguish between a loss and a win. And if the military cannot distinguish between those, then it will have a seriously unbalanced understanding of cyber power.

B. US – Iran, 2008 to 2015

Unfortunately, not all analyses of cyber conflict are as straightforward as that of Estonia. The ongoing cyber conflict between Iran and the United States has not just been a single campaign, but a years-long back and forth, with each side apparently giving as good as they've got.

Seemingly the first shot in the cyber conflict, at least from public sources, was the US-Israeli Stuxnet attack against Iranian uranium enrichment capability (Sanger, 2012). This first-ever truly destructive cyber attack, conducted from around 2008 onwards, was certainly a tactical

and operational success, destroying at least 1,000 centrifuges (Zetter, 2014). Whether or not it was a strategic win is harder to gauge, as Iranian enrichment actually increased during this period, though the cyber attack did perhaps help forestall an Israeli air strike.

Unfortunately, Stuxnet was an operational success that forced the Iranians to redouble their own cyber capabilities, which they had generally ignored until attacked (Fox-Brewster, 2014). In 2012, Iran appears to have conducted a massive and sustained denial-of-service attack against many US banks, including Bank of America, Citigroup, Wells Fargo, PNC and others, 'most likely in retaliation for economic sanctions and online attacks by the United States' (Perlroth and Hardy, 2013). The attacks were 'unprecedented' in 'scale, scope, and effectiveness' and seen as 'the first significant digital assault of its kind undertaken against American industry's computers by a foreign adversary' (Nakashima, 2014).

As the attacks were reported as 'major disruptions' and took place over months, they were probably considered a tactical and technical success; if the ultimate political purpose was to disable the entire finance sector or to coerce US policy towards Iran, then they fell far short. If, instead, the goal was retribution for sanctions or to attract the attention of US policy-makers, then perhaps the Iranians considered that they won that round.

At about the same time, another series of tit-for-tat attacks were taking place. Iran was forced, in April 2012, to disconnect some oil wells from the Internet in the face of the damaging Wiper worm, which wiped the hard drives of computers of several oil companies and bureaucracies (Erdbrink, 2012). According to most analyses, the attack was most likely the work of Israel, keen to disrupt the Iranian economy (Zetter, 2014). Just a few months later, in August, a nearly identical wiper attack, called Shamoon, took down nearly 30,000 computers at Saudi Aramco, and more a few days later at RasGas (Perlroth, 2012). A leaked NSA document meant for the NSA director, General Keith Alexander, 'suggests that the attack on Saudi Aramco was in response to 'a similar cyberattack' against Iran's oil industry earlier that year' (Sanger, 2015).

Shamoon has been called a 'game changer' even more significant than Stuxnet, as it was so destructive. But if the Iranian goal was to disrupt Saudi oil and Qatari gas production, then the attack was an operational and strategic flop. There was no disruption of production. American officials who point to Shamoon as a game changer might be technically correct, but are highlighting an attack which was not just a somewhat symmetrical retaliation but which largely failed.

On balance, the individual engagements – Stuxnet, bank DDoS attacks, Wiper, and Shamoon – were all tactical wins. Other than Stuxnet, most seem to have been operational defeats, or at least failures, as the damage inflicted was neither severe nor lasting enough. Not knowing what the political objectives were for Israel, Iran, or the United States, it is even harder to identify any strategic victor.

As a footnote, in the less combative atmosphere after the nuclear agreement with Western powers in 2015, Iran has shifted its cyber operations away from such destructive attacks to espionage (Bennett, 2015).

4. ANALYSIS

As in many other areas of warfare, tactical and technical gains seem relatively easy but translating those into larger political and military success is far harder. It is likewise easiest to determine the victor at the more tactical and technical levels.

A. Difficulty of assessing who won

At the strategic level, the question of 'who won' defies an easy binary answer, for many reasons: an over-focus on the tactical and technical levels of cyber operations; a military fascination with capabilities, especially usable ones; the nature of irregular conflicts; a lack of a national cyber strategy; and high security classifications.

Cyber conflict is also fought over networks using bits and bytes by cyber warriors who are steeped in technical know-how, so it is no surprise that winning or losing have been such a technical determination. Cyber conflict is indeed fast at the tactical level; ones and zeroes do indeed travel at network speed. But the public evidence is clear that individual engagements have rarely if ever made a strategic, national security difference (Lindsay, 2013; Healey, 2013).

Tied to this technical mind-set is a strong military focus, not on operations, doctrine, or strategy but on capabilities. Any time a military officer or leader discusses cyber capabilities, they are in some way reinforcing a tactical and technical mentality, fighting from the foxhole or an endless series of dogfights rather than with a larger picture. I have been in meetings with the most senior Air Force cyber officers where the discussion never got farther than what capabilities will set the Air Force apart from other services, rather than what cyber conflict of the future might be like and how the United States and its Air Force can prevail.

Cyber capabilities are seen as usable in an era when more overt military power is largely forbidden, so 'doing something' in a post-Vietnam, post-9/11 era becomes almost a political end in itself. Along with special forces (whether SEAL trainers or "little green men"), proxy non-state groups, or drone strikes, nations engage in offensive or espionage cyber operations for relatively limited tactical gains, divorced from longer-term strategic outcomes. Likewise, cyber conflicts tend to be irregular conflicts, and it is almost always difficult to determine winning or losing in such fuzzy and indistinct circumstances. Counter-terrorism experts voice the same frustrations on whether their successful operations are leading to an overall win or a loss. Likewise, determining if the United States or Iran won their cyber engagements is in some ways no more or less difficult than deciding if the United States is winning in Iraq, Afghanistan, or Syria. The goals of those conflicts have reduced significantly over the years, and winning and losing have been redefined many times.

This is especially difficult for the United States, as it does not have a single cyber strategy by which to assess victory or defeat. Rather, there are separate strategies for the military, commerce and trade, and international issues. The counterinsurgency warfare community has had a decades-long debate on whether winning was best pursued by winning the hearts and minds of the citizens or by killing the insurgents, so that tactics and operations could be

balanced against these larger goals. Lacking such a cyber strategy, the United States is hobbled in trying to answer critical questions such as whether risky attacks like Stuxnet are worth the danger. With so much post-9/11 power centred in the Pentagon, the military view of winning becomes the default.

In addition, nations ensure that their offensive and espionage cyber operations are highly classified. It is difficult for anyone other than a handful of extremely highly cleared military officers and senior officials to know which side is winning in the Iran versus US and Israel conflict. Worse, US cyber warriors classify or downplay any outgoing cyber attacks, then loudly denounce attacks or even counterattacks by the other side. The best examples involve Iran, where the US and Israel threw the first punch with Stuxnet. US officials like General Alexander later downplayed that attack, which nearly all other experts, including his predecessor as NSA Director, considered to be 'crossing the Rubicon' into a new era of cyber conflict (Sanger, 2012), to rather highlight the Iranian Shamoon attack (InfoSec Magazine, 2014). But Shamoon was in fact apparently a relatively proportionate retaliation to the earlier Wiper attack on Iran's own energy industry. Listening only to statements by General Alexander might lead experts to believe that the United States was losing to an aggressive Iran.

B. Toward a better understanding of winning

These reasons make it difficult to think clearly about winning or losing in cyber conflict, but there is still room for significant progress. Cyber warriors tend to see that Estonia lost in 2007 because of a focus on technical impact rather than the more strategic view that winning means achieving better national security outcomes. Estonia won because it emerged from 2007 far stronger and has spent the better part of a decade building on that strength; Russia came out weaker relative to Estonia, NATO, and other perceived adversaries.

Accordingly, the most important next step for many nations facing cyber conflict is to be far clearer about preferred national security outcomes; these should be prioritised in a clear national cyber strategy to clarify decisions when a government is faced with competing public goals.

Those national security outcomes might define winning in different ways:

- **Hard-power perspective:** Winning in cyberspace is dominating it for espionage and offensive operations, with the best arsenal of cyber capabilities and 'collecting the whole haystack' of worldwide ones and zeros, as one official described the NSA approach (Nakashima & Warrick, 2013).
- **Soft-power perspective:** Winning in cyberspace is to seize this once-in-a-century opportunity to win the hearts and minds of the digital natives in whatever nation they live, so that they see our nation as representing their values and enriching their lives, giving concomitant influence.
- **Economic-power perspective:** 'Winning in cyberspace' is to have the most agile Internet-enabled economy, the strongest technology companies, and the most trusted cyber security experts.

If the militarised view of long-term national security outcomes turns out to be the historically correct perspective, then nations like the United States and Russia are on a strong path. If, however, either the soft-power or economic perspectives are likely to lead to better outcomes, then the United States and nations that copy its views on cyber power are headed for potentially far worse outcomes.

Nations which follow the hard-power perspective are likely to win battles, but never the war.

5. RECOMMENDATIONS

Cyber espionage and attack are ultimately perhaps too ingrained as modern tools of statecraft to see a drastic reduction, especially to other forms of irregular conflict. For example, if a head of government wanted to ban assassinations (as President Gerald Ford did in 1976) or stop using drones for targeted killing of terrorists, the decision and execution are relatively straightforward; they have but to say that these actions are not in the long-term interest of the nation, and direct that they stop. With nearly the whole world being wired, it is now the 'golden age of espionage' for intelligence services using cyber means, while militaries see adversaries increasingly adding networking capabilities to ever more juicy-looking targets. Few heads of government could simply demand that it all stop. Accordingly, solutions are more about the degree of emphasis and process.

To align around a better view of using cyber power to win, nations – starting with the United States – need to take the following actions:

1. **Create an overarching cyber strategy** that is clear about which long-term national cyber priority is the most important: hard power, soft power, or economic power. Strategies cannot, as has often been the norm in the United States and other nations, list multiple competing priorities pursuing often competing public goods. This document should be driven, and signed, by the head of government. If a full 'strategy' is too difficult for bureaucratic or other reasons, just a clearly delivered policy preference by the head of government can be sufficient.
2. **Revamp the interagency policy process** to deliver on the priority chosen to deliver those long-term best outcomes. For example, major military or espionage campaigns cannot be shielded from scrutiny for classification reasons, or approved by only a narrow base of cleared individuals often with little experience or concern of non-military or -intelligence matters.
3. **Encourage a broader understanding of cyber power**, including how future cyber conflict might differ from what is seen today; the interplay of soft power and economic power on the results of cyber conflict; the role of the private sector in delivering victory; and the differences between the tactical, operational and strategic levels of cyber conflict. With the current mind-set so ingrained in many governments and militaries, this broader dialogue probably needs to be led by academia and think tanks, perhaps supported by grants.

4. **Promulgate broader thinking in subordinate strategies and doctrine**. The view of 'victory' that is decided on by governments needs to trickle down into the bureaucracy, especially into individual ministries' cyber strategies and projects, military strategy and doctrine, and into military academies so that the next generations of military practitioners and leaders learn the best way to do things, not the merely the past and current way.

It is apparent that there is a deep misunderstanding of what constitutes victory in cyber conflict, with far too much attention on actions on the network and not on actual national security outcomes. This is most apparent in the Estonia cyber conflict of 2007, widely seen in the US military as a defeat, but which was in fact a fairly crushing operational and strategic win for the Estonians.

Cyber power is becoming far too important for such a fundamental misunderstanding, where a victory is mistaken for a defeat. Fortunately, there is a relatively straightforward set of recommendations, starting with a clear national priority set by the head of government, which clearly points to a clearer path.

REFERENCES

Alexander, Gen Keith, interview by Christopher Joye. 2014. 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander' *Financial Review*, May 9. http://www.afr.com/technology/web/security/interview-transcriptformer-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140507-itzhw.

Alexander, Keith, interview by Jason Healey. 2013. (May 3).

Barzashka, Ivanka. 2013. 'Are Cyber-Weapons Effective?' *RUSI Journal* (Royal United Services Institute) 158 (2).

BBC News. 2007. 'Putin in veiled attack on Estonia' May 9. http://news.bbc.co.uk/2/hi/europe/6638029.stm.

Bennett, Cory. 2015. 'Iran launches cyber offensive after nuclear deal'. *TheHill.com* November 24. http://thehill.com/policy/cybersecurity/261190-iran-switches-to-cyber-espionage-after-nuclear-deal.

Bumiller, Elisabeth, and Tom Shanker. 2012. 'Panetta Warns of Dire Threat of Cyberattack on U.S.' *New York Times* October 11. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0.

Deloitte. 2015. *Winning the Cyber War*. London: Deloitte. http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consultancy/deloitte-uk-symantec-deloitte-partnership-uk.pdf.

Economist. 2010. 'War in the fifth domain.' *The Economist*, June 1. http://www.economist.com/node/16478792.

Economist. 2012. 'Paper Cuts.' *The Economist*. October 27. http://www.economist.com/news/international/21565146-paperless-polling-stations-are-unfashionable-internet-voting-its-way-paper-cuts.

Erdbrink, Thomas. 2012. 'Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet.' *New York Times*. April 23. http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html?_r=0.

Fox-Brewster, Thomas. 2014. '"Bone-Chilling" Research Suggests Iran Gearing Up To Avenge Stuxnet Hacks.' *Forbes.com* December 2. http://www.forbes.com/sites/thomasbrewster/2014/12/02/bone-chilling-research-suggests-iran-gearing-up-to-avenge-stuxnet-hacks/.

Gartzke, Eric. 2013. 'The Myth of Cyberwar.' *International Security* 41-73. http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136.

Gambill, Gary. 2000. 'Who's Winning the Arab-Israeli Cyber War?' November. https://www.meforum.org/meib/articles/0011_me2.htm.

Gonzalez, Eileen. 2014. 'Retired General: Sony cyber attack is an act of war'. December 2. http://www.ksat.com/news/retired-general-sony-cyber-attack-is-an-act-of-war.

Healey, Jason, ed. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.

Healey, Jason. 2013. 'Concluding Assessment.' In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, by Jason Healey. Cyber Conflict Studies Association.

Healey, Jason, and Klara Tothova Jordan. 2014. *NATO's Cyber Capabilities: Yesterday, Today and Tomorrow*. Issue brief, Atlantic Council. http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf.

Infosecurity Magazine. 2014. 'Saudi Aramco Cyber Attacks a 'wake-up call', Says Former NSA Boss'. May 8. http://www.infosecurity-magazine.com/news/saudi-aramco-cyber-attacks-a-wake-up-call-says/.

IP Theft Commission. 2013. *Report on the Commission on the Theft of American Intellectual Property*. National Bureau of Asian Research. http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

Kay, Kim. 2015. *How to Win the Cyber War*. November 30. http://wwpi.com/how-to-win-the-cyberwar/.

Khanna, Parag. 2015. 'How small states prepare for cyber-war'. *CNN.com* September 2. http://www.cnn.com/2015/09/02/opinions/estonia-cyber-war/.

Kuehl, Dan, and Robert A Miller. 2009. *Cyberspace and the 'First Battle' in 21st Century War*. Washington DC: National Defense University Press. http://ndupress.ndu.edu/Portals/68/Documents/defensehorizon/DH-68.pdf.

Kuehl, Daniel. 2009. 'From cyberspace to cyberpower: Defining the problem.' In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr and Larry Wentz. National Defense University.

Lindsay, Jon. 2013. 'Stuxnet and the Limits of Cyber Warfare.' *Security Studies*. http://www.tandfonline.com/doi/pdf/10.1080/09636412.2013.816122.

Mite, Valentinas. 2007. 'Estonia: Attacks seen as first case of "cyberwar"'. May 30. http://www.rferl.org/content/article/1076805.html.

Nakashima, Ellen. 2014. 'U.S. rallied multinational response to 2012 cyberattack on American banks'. *Washington Post* April 11. https://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html.

Nakashima, Ellen, and Joby Warrick. 2013. 'For NSA chief, terrorist threat drives passion to "collect it all"'. *Washington Post* July 14. https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.

Nanjappa, Vicky. 2010. 'Cyber wars: Pak has an advantage over India'. *Rediff.com* August 16. http://www.rediff.com/news/report/indo-pak-cyber-war-set-to-escalate/20100816.htm.

Nye, Joseph. 2010. *Cyber Power*. Harvard Kennedy Schook, Belfer Center. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

Perlroth, Nicole. 2012. 'In Cyberattack on Saudi Firms, U.S. Sees Iran Firing Back'. *New York Times* October 23. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

Perlroth, Nicole, and Quentin Hardy. 2013. 'Bank Hacking Was the Work of Iranians, Officials Say'. *New York Times* January 8. http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=1.

Rattray, Gregory. 2001. *Strategic Warfare in Cyberspace*. MIT Press.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford University Press.

Roberts, Thomas. 2015. 'Is Anonymous' cyber war against ISIS working?' November 23. http://www.msnbc.com/thomas-roberts/watch/is-anonymous-cyber-war-against-isis-working-572660291779.

Sanger, David. 2015. 'Document Reveals Growth of Cyberwarfare Between the U.S. and Iran'. *New York Times* February 22.

Sanger, David. 2012. 'Obama Order Sped Up Wave of Cyberattacks Against Iran'. *New York Times* June 1. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

Schmidt, Andreas. 2013. 'The Estonian Cyberattacks.' In *A Fierce Domain: Cyber Conflict, 1986 to 2012*, by Jason Healey. Cyber Conflict Studies Association.

Singh, Ritu. 2015. 'Cyber-war: Indian hackers hack 250+ Pakistani websites after attack on Kerala govt's website'. ZeeNews September 29. http://zeenews.india.com/news/net-news/cyber-war-indian-hackers-hack-250-pakistani-websites-after-attack-on-kerala-govts-website_1803606.html.

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

US China Commission. 2008. *US China Commission 2008 Annual Report*. US GPO. http://origin.www.uscc.gov/sites/default/files/annual_reports/2008-Report-to-Congress-_0.pdf.

US China Commission. 2015. *US China Commission 2015 Annual Report*. US GPO. http://origin.www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF.

US Department of Defense. 2013. *Joint Publication 3-12, Cyberspace Operations*. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Valeriano, Brandon, and Ryan Maness. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown.