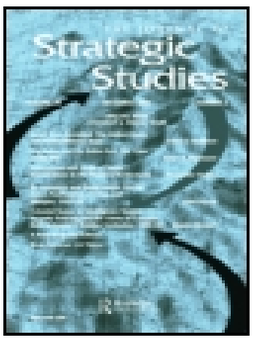

Journal of Strategic Studies

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fjss20

Cyber campaigns and strategic outcomes

Richard J. Harknett & Max Smeets

To cite this article: Richard J. Harknett & Max Smeets (2020): Cyber campaigns and strategic outcomes, Journal of Strategic Studies, DOI: 10.1080/01402390.2020.1732354

To link to this article: https://doi.org/10.1080/01402390.2020.1732354

Published online: 04 Mar 2020.

JOURNAL OF STRATEGIC STUDIES
https://doi.org/10.1080/01402390.2020.1732354

Routledge
Taylor & Francis Group

ARTICLE

OPEN ACCESS Check for updates

Cyber campaigns and strategic outcomes

Richard J. Harknett[a] and Max Smeets[b]

[a]Department of Political Science, University of Cincinnati, Cincinnati, OH, USA; [b]ETH Zurich Center for Security Studies Digital Library, Zurich, Switzerland

ABSTRACT

While much focus has remained on the concept of cyberwar, what we have been observing in actual cyber behaviour are campaigns comprised of linked cyber operations, with the specific objective of achieving strategic outcomes without the need of armed attack. These campaigns are not simply transitory clever tactics, but strategic in intent. This article examines strategic cyber competition and reveals how the adoption of a different construct can pivot both explanation and policy prescription. Strategy must be unshackled from the presumption that it deals only with the realm of coercion, militarised crisis, and war in cyberspace.

KEYWORDS Cyberwar; cyber campaigns; cyber operations; cyber espionage; China; Russia

Introduction

Over the course of the last three decades, and increasingly over the past eight years, behaviour in cyberspace is veering in a direction that much of cybersecurity literature did not.[1] Whereas much of the academic and policy communities' focus was on 'the high-and-right' cyber equivalent to an armed attack, captured in the concept of cyberwar, the actual behaviour of actors has been of a far more nuanced and different nature. Significantly, what has emerged are campaigns comprised of linked cyber operations, with the specific objective of achieving strategic outcomes without the need of armed attack. These campaigns are not simply transitory clever tactics. Rather, they are persistent responses to the structural imperatives of cyberspace itself as a domain and as such we can anticipate that they will be the central mechanism of state and semi-state competition in this realm as long as the core structure of cyberspace endures. This article posits that the

CONTACT Richard J. Harknett richard.harknett@uc.edu

[1]Egloff uses the term semi-state actors to describe cyber agents that work closely with state decision-makers but are not directly under state control. Examples such as Huawei and Kaspersky have been considered by western countries as private companies that appear to act intertwined closely with their home government. Florian Egloff, 'Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates'. DPhil Thesis, University of Oxford, 2018; Also see Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press 2018).

fundamental nature of cyberspace rests on a structure of interconnectedness and a condition of constant contact. Once recognised, that structural environment requires us to study cyber means not as enablers of war, although they can be, but more critically as the strategic alternative to it.

This article puts forth the central argument that cyberspace has opened a new dimension of power politics in which cyber campaigns could potentially become a salient means, alternative to war, for achieving strategic advantage. Whereas cybersecurity policy and academic study has tried to deal with the prospect of cyber means enabling traditional Clausewitzian notions of combat, it is time that we assess a second category of significant interaction – one that involves the prospect of achieving strategic ends without the resort to war. The true strategic consequence of cyber means may lie not in producing the catastrophic armed attack that disables a country in a surprise moment, but the fact that cyber means can affect sources of national power without such attack.

The purpose of this article is not to evaluate different policies, but through a reflection on the fundamental nature of cyber competition show how the adoption of a different theoretical lens can pivot both explanation and policy prescription. We offer the proposition that strategy must be unshackled from the presumption that it deals only with the realm of coercion, militarised crisis and war in cyberspace. Cyber competition is *strategic* in its intent to shift the relative balance of national power among states. If this proposition holds, it can unlock new avenues for security studies research and will require different policy responses. The remainder of this article is outlined as follows. Section II discusses the bias towards a focus on cyberwar as a variant of armed attacks that are highly disruptive or destructive in nature and may cripple society directly. Section III explains the need to realign the literature and focus on cyber operations, amalgamated into cyber campaigns, which often take place below the threshold of armed attack whilst seeking to achieve strategic advantage. Section IV brings in the empirics and specifically focuses on a heuristic case study of how Chinese cyber operations affect sources of national power. Section V takes up possible objections to the claims made in the previous section and explains why activity below the threshold of armed attack is not merely sporadic and should be distinguished from intelligence activity. The final section, Section VI, concludes and discusses avenues for future research.

The 'high-and-right' bias in the cyberwar literature

To grasp the revolutionary potential of cyberspace, the academic and policy communities have paid particular attention to the possible disruptive or

destructive nature of cyber attacks.[2] The first part of this section examines the emergence of this literature. The second part explains the limitations of this debate in understanding the true potential of cyberspace to affect power politics.

The cyberwar debate

For more than two decades, the literature has debated if, when, and how cyberwar will occur. The literature on cyberwar can be divided into multiple phases.[3] In 1993, John Arquilla and David Ronfeldt initiated the scholarly debate on the coming of cyberwar, talking about how information and communications systems could be disrupted or even destroyed when the United States ends up in a new militarised conflict.[4] In the mid-1990s, influenced by the Oklahoma City Bombing, the meaning of the concept and discussion on cyberwar made a turn.[5] The cyberwar debate no longer focused on the disruption of information and communication systems on the battlefield, but became increasingly associated with the potential crippling of society's critical infrastructure.[6] The Distributed

[2]On the discourse of policymakers about the crippling of critical infrastructure through cyber attacks see: Myriam Dunn Cavelty, *Cyber-Security and Threat Politics US Efforts to Secure in the Information Age* (Abingdon: Routledge 2008); Ralf Bendrath, 'The American cyber-angst and the real world – any link?' Paper presented at: International Studies Association Annual Convention, University of Bremen (2004) p. 72; Ralf Bendrath, 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection', *Information & Security* 7, (2001), 80–103; Helen Nissenbaum, 'Where Computer Security Meets National Security', *Ethics and Information Technology*, 7/2 (2005), 61–73; Rachel Yould, 'Beyond the American Fortress: Understanding Homeland Security in the Information Age', in Robert Latham (ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security* (The New Press 2003).

[3]For a more comprehensive overview, see: Jason Healey and Karl Grindal, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association 2013).

[4]Their vision about the need for information dominance on the battlefield was said to be less inspired by the U. S. victory in the Gulf War against Iraq, and more by the fighting of the Mongol Empire of the 13th century – as their success was largely based upon superior communication of the field commanders. John Arquilla and David Ronfeldt, 'Cyberwar is coming!' *Comparative Strategy* 12/2 (1993), 141–65; also see John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: The Rand Corporation); John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica: Rand Corporation 2001).

[5]In response to the tragedy, the President's Commission on Critical Infrastructure Protection (PCCIP) was formed by the Clinton administration. The Commission released its report to President Clinton in October 1997, examining both the physical and cyber threats to the nation. Although the commission did not 'discover[. . .] an immediate threat sufficient to warrant a fear of imminent national crisis, it did find reasons to implement new measures, especially in the area of cyber security. As a product of the Commission's report, President Clinton released Presidential Decision Directive 63 (PDD-63) in May 1998. PDD-63 called for a range of actions intended to improve the nation's ability to protect 'critical infrastructure' from physical and cyber-attacks; President's Commission on Critical Infrastructures, 'Infrastructure Protection, Critical Foundations: Protecting America's: The Report of the President's Commission on Critical Infrastructure Protection', (13 October 1997), https://www.fas.org/sgp/library/pccip.pdf, Ibid, p.x; The White House, 'The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive', *White Paper*, 63 (22 May 1998), www.fas.org/irp/offdocs/paper598.html.

[6]As David Betz and Tim Stevens also note about the (recent) cyberwar debate: 'Popular discourse on cyberwar tends to focus on the vulnerability of the "physical layer" of cyberspace to cyber-attack and the ways in which this may permit even strong powers to be brought to their knees by weaker ones, perhaps bloodlessly'. David J. Betz and Tim Stevens, 'Cyberspace and the State: Towards a Strategy for Cyber-Power', *Adelphi Series*, 51/424 (2011), 75–98, 76.

Denial of Service (DDoS) attacks against Estonia (2007) and Georgia (2008) as well as the discovery of Stuxnet (2010), the malicious computer worm targeting the nuclear centrifuges in Natanz, Iran encouraged a deepening of this focus.[7]

This led to two opposing camps with firmly entrenched positions about cyberwar.[8] For some, cyberwar is real – and may already be upon us. Mike McConnell, former Director of National Intelligence and the National Security Agency (NSA), wrote in an article that 'we have entered a new age of threat, defense, deterrence and attack equivalent in some ways, to the atomic age. Cyberattacks have the potential to damage our way of life as devastatingly as a nuclear weapon'.[9] Clarke and Knake describe a vivid scenario of a cyber-attack that causes a power blackout in metropolitan areas, the burning of oil-supplies, a freeze in the financial system, and the explosion of pipelines.[10] Gary McGraw opens his article on why *Cyber War is Inevitable (Unless We Build Security In*):

> Information systems control many important aspects of modern society, from power grids through transportation systems to essential financial services. These systems are riddled with technical vulnerabilities. Consequently, our reliance on these systems is a major factor making cyber war inevitable, even if we take into account (properly) narrow definitions of cyber war. The cyber environment is target rich and easy to attack. Even weak actors can have a

[7]On Estonia see: Eneken Tikk, Kadri Kaska and Liis Vihul, 'International Cyber Incidents: Estonia 2007 (Tallinn: NATO CCDCOE 2010) 14–25, p. 33; in Ottis, 'Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective', *Proceedings of the 7th European Conference on Information Warfare and Security* (Plymouth: Academic Publishing Limited 2008), 163–68; On Georgia see: Eneken Tikk, Kadri Kaska and Liis Vihul, 'Cyber Attacks Against Georgia', (Tallinn: NATO CCDCOE 2008); Paulo, Shakarian, 'The 2008 Russian Cyber Campaign Against Georgia', *Military Review* (2011, November–December), p. 63–64; Ronald J. Deibert, 'Cyclone in cyberspace: information shaping and denial in the 2008 Russia-Georgia war', *Security Dialogue* 43 (2012), 3–24; David M. Hollis, 'Cyberwar case Study: Georgia 2008', *Small Wars Journal*, (2011, January); On Stuxnet see: Michael Joseph Gross, 'A Declaration of Cyber-War', *Vanity Fair* (2011, April); James P. Farwell and Rafal Rohozinski, 'Stuxnet and the future of cyber war', *Survival: Global Politics and Strategy* 53/1 (2011), 23–40; David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American* Power (New York: Crown: 2012), 188–209; Dorothy E. Denning, 'Stuxnet: What Has Changed?' *Future Internet*, 4 (2012), 672–87; Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (2014), CBS News, 'Stuxnet: Computer Worm Opens New Era of Warfare', 60 Minutes (4 March 2012); Ralf Langner, 'Stuxnet: Dissecting a Cyberwarfare Weapon', *Security and Privacy* 9/3 (2011) 49–51; Jon Lindsay, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, 22/3 (2013), 365–404; Sean Collins and Stephen McCombie, 'Stuxnet: the emergence of a new cyber weapon and its implications', *Journal of Policing, Intelligence, and Counter Terrorism* 7/1 (2012), 80–91; Less attention was paid to other disruptive and destructive capabilities such as Witty Worm (2004), Hacking Scientology (2008), Dozer (2009), Koredos (2010), and Groovemonitor (2012). More recently, much has been written on the Sony/Destover (2014), Shamoon (2012), Ukraine attacks (2015), Shamoon 2.0 (2016), and NotPetya (2017).

[8]This is not to say that cyberwar discussion has been further refined over the years, with scholars talking in more detail about the destructive potential of cyber attacks, the costs to conducting cyber attacks, the offence-defence balance, and the diffusion of capabilities. Also, this position was held in both the scholarly literature (the primary focus of this discussion) as well as in policy documents (see for example, 2010 National Security Strategy).

[9]Mike McConnell, 'Cyberwar is the New Atomic Age', *New Perspectives Quarterly* 26/3 (Summer 2009).

[10]Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: Ecco 2010); for a similar statement see: Leon E. Panetta, 'Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City', *News Manuscript U.S Department of Defense*, (2012, October) http://www.defence.gov/transcripts/transcript.aspx?transcriptid=5136

> major asymmetric impact. The only solution is to improve our cyber defenses by designing and implementing secure software.[11]

Other scholars and analysts are more sceptical – observing a striking absence of physical violence in the type of attacks that are conducted in cyberspace. Thomas Rid argues that cyberwar has not and will not occur.[12] According to Rid, no cyberattack meets all three of Clausewitz' criteria of war as 'violent', 'instrumental' and 'political'.[13] Instead, Rid concludes 'all past and present political cyber attacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage'.[14] Erik Gartzke joins Rid in arguing that cyberattacks have not brought much of a transformation, dubbing cyberwar a 'myth'.[15] Also drawing upon the work of Clausewitz, Gartzke concludes that '[t]he internet is generally an inferior substitute to terrestrial force in performing the functions of coercion or conquest. Cyber "war" is not likely to serve as the final arbiter of competition in an anarchical world and so should not be considered in isolation from more traditional forms of political violence'.[16] Adam Liff, sets up a different framework for assessing cyberwar than Rid and Gartzke but largely arrives at the same conclusion: it is unlikely that cyberwarfare is the new 'absolute weapon'.[17] He concludes that '[c]yberwarfare appears to be a tool for states to pursue political (strategic) and/or military (tactical) objectives at relatively low cost only under very limited circumstances. Although Stuxnet manifests cyberwarfare's potential to become a useful brute force measure, no examples of irrefutably effective coercive CNA [Computer Network Attack] exist'.[18] Martin Libicki notes that 'operational cyberwar' – that is, cyberattacks that facilitate a combat operation – may have an important niche role, but not

[11]For other works drawing upon this cyberwar notion also see: Arquilla, John, Rebuttal Cyberwar Is Already Upon Us, *Foreign Policy;* Mar/Apr 2012; 192; ProQuest pg. 84; Gary McGraw, 'Cyber War Is Inevitable (Unless We Build Security In)', *Journal of Strategic Studies* 36/1 (2013), 109–19. http://doi.org/cp6f

[12]Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35/1 (2012), 5–32; also see: Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press 2013); Thomas Rid, 'Think Again: Cyberwar', Foreign Policy, 27 February 2012, http://foreignpolicy.com/2012/02/27/think-again-cyberwar; Rid, Thomas, 'Is Cyberwar Real?' in response to Jarno Limnéll Foreign Affairs, March/April.

[13]In fact, the scholar notes that most cyberattacks do not even meet one of these criteria. For a similar analysis, also drawing upon these three elements see: Thomas G. Mahnken, 'Cyber War and Cyber Warfare', in Kristin Lord and Travis Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. 2 (Washington DC: CNAS 2011), 53–62.

[14]Rid, 'Cyber War Will Not Take Place'; for a theory driven response to Rid see: John Stone, 'Cyber War Will Take Place!' *Journal of Strategic Studies* 36/1 (2013) 101–08.

[15]As Gartzke concludes: 'Even the most successful forms of cyberwar (such as cyber espionage) do not presage much of a transformation'. Erik Gartzke, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', *International Security*, 38/2 (2013), 41–73.

[16]Gartzke, 'The Myth of Cyberwar'.

[17]Adam P. Liff, 'Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War', *Journal of Strategic Studies* 35/3 (2012), 401–28; Also see: Timothy J. Junio, 'How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate', *Journal of Strategic Studies* 36/1 (2013), 125–33; Adam P. Liff, 'The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio', *Journal of Strategic Studies* 134–38.

[18]Liff, 'Cyberwar', 426.

much more.[19] Libicki is even less convinced that 'strategic cyberwar' – cyber-attacks which determine the outcome of war or 'state policy'- will occur in the future.[20] Finally, Valeriano and Manness study the dynamics of cyber conflict across rivals between 2001 and 2011. Their main conclusion is that rivals are engaging in cyber conflict, that is rarely coercive and primarily restrained: the actual magnitude and pace of cyber disputes among rivals does not match with popular perception.[21]

Beyond cyberwar

Whilst the focus of academic debate has been whether cyber activity can reach the threshold of war, in reality, the behaviour of state and non-state actors has been of a different nature. Most of this behaviour has been referred to as malicious cyber activity and sub-categorised as 'cyber espionage', 'hacktivism', 'sabotage', 'cybercrime' and even 'cyber terrorism'.

Yet, this view and type of categorisation does not lend itself well to understanding how and, more importantly, why key actors are operating in cyberspace and, in fact, it leads to a distortion in the studying of cyber operations. The bias has been to consider 'war' as the only critical concern and thus the debate over whether a cyber operation on its own can constitute war appeared as the key issue to resolve.[22] The implication of the terminology (and the study to date) of everything else that clearly is not crossing the threshold of armed attack equivalence is that it is more tactical at best – the term malicious, itself, implies something more in the realm of nuisance than of critical importance. One must ask then, why are so many actors engaging in so much of this 'malicious' activity if it really does not

[19]Martin Libicki, *Cyberwar and cyberdeterrence* (Santa Monica: RAND Corporation 2009). https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf; also see: Libicki, Martin C., 'Cyberspace is Not a Warfighting Domain', *I/S A Journal of Law and Policy for the Information Society* 8/2 (2012), 325–40. http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf

[20]As Libicki notes 'can strategic cyberwar induce political compliance the way, say, strategic airpower would? Airpower tends to succeed when societies are convinced that matters will only get worse. With cyberattacks, the opposite is more likely. As systems are attacked, vulnerabilities are revealed and repaired or routed around. As systems become more hardened, societies become less vulnerable and are likely to become more, rather than less, resistant to further coercion'. Libicki, Cyberwar and cyberdeterrence, p. xv.

[21]Brandon Valeriano and Ryan C. Maness, 'The dynamics of cyber conflict between rival antagonists, 2001–11', *Journal of Peace Research* 51/3 (2014), 347–60; also see: Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, (New York: Oxford University Press 2015); also see: Richard Harknett, 'Review of Brandon Valeriano, Benjamin M. Jensen, Ryan C. Maness, Cyber Strategy: The Evolving Character of Power and Coercion', *H-Net Reviews in Social Science*, (2018 October) 1–3.

[22]The distortion is broader than just technically the absence of war in that Gartzke, Rid, Borghard and Lonegran and others have assessed cyber operations expecting them to be coercive tools, but there is no indication empirically that states using cyber operations principally as coercive means. Rather, the record suggests that cyber campaigns are being assembled to directly (cumulatively) adjust relative power through relative gains and losses. See: Erica D. Borghard and Shawn W. Lonegran, 'The Logic of Coercion in Cyberspace', *Security Studies* 26/3 (2017), 452–81; Gartzke, 'The Myth of Cyberwar'; Rid, 'Cyber War will not take place'.

amount to very much? It could be that cyber means simply make stealing, whether for criminal goals or spying purposes, and one-off disruptions of activities a lot easier, so it is happening more frequently. If this is the case, not much further research out of the field of security studies is likely warranted.

An alternative hypothesis is that this scale and scope of cyber activity is being driven with an intent to achieve strategic advantage – to actually shift the distribution of power without having to use war as the primary means. If the prospect that cyber activity *below* the threshold of armed attack can produce a strategic outcome holds, then this sustained activity does rise to the level of importance for further academic explanation and study. Is it possible that the Gartzke thesis, among others, is both correct and misplaced? That is, it is correct to conclude that what we are experiencing is not war nor coercion, but that such a conclusion misses the point that war and coercion are not the only means by which states can pursue strategic advantage given the opportunities that cyberspace affords. Pursuing the fundamental question, 'what if', is the intellectual prospect to which the next section turns.

Redirecting the literature: A theoretical understanding of cyber campaigns and strategic advantage

What if the relationship between cyber operations (means) and strategic advantage (ends) has historically been explored in too narrow a manner? How should the literature be realigned to address the reality of actual cyber behaviour? How can we move beyond the cyberwar paradigm? Such a realignment rests first on a change in operationalising 'malicious' activity. While a proportion of cyber activity is of a lower end criminal nature or basic forms of reconnaissance and information-gathering, we must create within this empirical record the additional classification of coherent cyber campaigns. Instead of treating each cyber incident in isolation from one another, analytically we must capture some of those incidents as actual coordinated efforts within a larger planning construct. This shift in operationalising the activity then allows for the analysis to proceed as to whether a series of linked cyber operations – defined as a strategic campaign – can degrade or enhance sources of relative national power, without rising to the level of armed attack. Of course, secondarily, it also allows analysis of the conditions that lead to successful shifts in relative power, in that one might find that actors are engaged in cyber operations with strategic intent, but do not actually achieve the advantage they are seeking. This readjustment in how to look at the activity before us, thus, offers the opportunity to both explain the actor's behaviour and to assess the utility of that behaviour. It is not a simple semantic change but introducing the concept of cyber campaigns below the threshold of armed attack suggests a higher level of analytical precision that could be employed in the policies and strategies of many countries that

tend to still use variations of 'malicious cyber activity' as a catch-all for a range of cyber incidents that they fail to differentiate. A classification of some of this cyber activity as coordinated campaigns with strategic intent offers the policy community a prioritisation matrix that to date has been lacking when the categories have been essentially only war and not-war.

Cyber campaigns

There is a tendency to treat terms such as 'breach', 'cyberattack', 'hack', 'cyber incident' and 'cyber operation' as synonymous, whilst in reality, they have different meanings and connotations.[23] For the purposes of this study, it is especially important to carefully distinguish between 'cyber operations' and 'cyber campaigns'. A *cyber operation* refers to a series of coordinated actions directed towards a computer or network in order to achieve a certain operational objective.[24] The operational objectives of cyber operations are diverse.[25] One goal of cyber operations may be espionage – such as the theft of personal data or intellectual property. Cyber operations may also be conducted to cause disruption, denial, degradation, or destruction. Finally, a cyber operation may serve to defend a network from being exploited or attacked. A single cyber operation might have multiple and changing goals. For example, given the similarity in (initial) operational execution, an intelligence collection operation might turn into an operation which seeks to cause disruption or could lead to a remediation of a vulnerability that an adversary has discovered but not yet exploited.[26] The tactics of cyber operations – e.g. the planning and execution – also vary.

A *cyber campaign* refers to a series of coordinated cyber operations, which take place over time, to achieve a cumulative outcome leading to strategic advantage. Cyber operations, as part of a campaign, can be conducted against different actors and by different actors. For example, design plans of missile defence systems – and related technology – may be stolen from various defence corporations scattered across multiple countries. Yet, together, they are part of a larger campaign that helps a certain state to leapfrog military development in this area (in either strengthening their own ability to defend or to design around the defences of others or both). Cyber operations do not have to be conducted by the same threat actor to be part

[23]These different meanings – and implications – may differ across communities. For example, there are important legal connotations for calling certain cases a 'cyberattack'. There are equally important connections for computer security experts between 'hack' and 'breach'.

[24]Definition is based on: Matthew Monte, *Network Attacks and Exploitation: A Framework*, (Indianapolis: Wiley 2015).

[25]The U.S. intelligence community distinguishes between three types of Computer Network Operations (CNO): Computer Network Exploitation (CNE), Computer Network Attack (CNA), and Computer Network Defense (CND). Ibid.

[26]Michael Hayden, *Playing the Edge: American Intelligence in the Age of Terror*, (New York City: Penguin Random House 2016).

of the same campaign. Indeed, one could conceive of two or more separate threat groups, which conduct different types of cyber operations against a diverse set of targets but are part of the same cyber campaign.[27] Finally, cyber operations can enable or reinforce non-cyber operations leading to strategic outcome. For example, a cyber operation might gain access to administrative files of a terrorist group, such as payrolls and purchase records. This information could subsequently support a larger campaign using 'non-cyber means' to dismantle the terrorist organisation.

The duration of cyber campaigns can vary dramatically. Whereas some campaigns may last for years – based on numerous operations with large intervals between each – other campaigns have a much shorter time span.[28] Furthermore, the direct outcome of a cyber campaign does not necessarily lead to an *immediate* strategic outcome. At times, an actor can even have the opportunity to unlock the strategic value of its earlier operation at a time of their choosing. For example, if an adversary is able to collect a large trove of personal data of people who live in a certain country, this information might be valuable for future strategic objectives (data on surnames, nationality, children, place of birth, gender, are all unlikely to change over the years).[29] Finally, not all cyber campaigns are (and have to be) equally coordinated.[30]

The construct of campaigns with strategic intent offers a different assessment tool to explain behaviour and prescribe policy than constructs such as grey space or unpeace.[31] It is not just that we observe a great deal of activity below the threshold of armed attack; it this activity can intentionally have cumulative effects. These are not mere isolated events. What cyber means appear to enable is capacity to piece together more continuously and more seamlessly at significant speed and scope activities that vary in their

[27]For an example see: See: James Scott and Drew Spaniel, 'China Espionage Dynasty: Economic Death by A Thousand Cuts', *Institute for Critical Infrastructure Technology*, (28 July 2016), http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.07.28.China_Espionage_Dynasty/ICIT-Brief-China-Espionage-Dynasty.pdf.

[28]For a particularly long campaign see Moonlight Maze. Using a UK company's vintage web server kept in storage for over 20 years, researchers were able to connect the 1990 s 'Moonlight Maze' operations against the US government to the 'Turla' activity from the 2000 s (Turla is still active today). According to one of the researchers, 'The Moonlight Maze group stripped away components that didn't work and combined tools that did to make them more potent. And unlike modern hacking operations that use a lot of automated scripts, the Moonlight Maze operators did everything in real time'. See: Kim Zetter, 'New Evidence Links a 20-Year-Old Hack on the US Government to a Modern Attack Group', *Motherboard*, (3 April 2017), https://motherboard.vice.com/en_us/article/vvk83b/moonlight-maze-turla-link; Juan Andres Guerrero-Saade, Costin Raiu, Daniel Moore, Thomas Rid, 'Penquin's Moonlit Maze: The Dawn of Nation-State Digital Espionage', Kaspersky Lab, (2018), https://media.kaspersky contenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf.

[29]For a more detailed discussion of the OPM hack see section IV.

[30]For example, long-term disinformation campaigns require much less coordination than long-term IP theft. In the former case, the spread of false information can come from multiple, different sources. When and what is distributed is not always of great importance to the success of the campaign. In the latter case, there needs to be a sizeable 'coordination apparatus' which is able to turn the collected input into meaningful output.

[31]Lucas Kello, *The Virtual Weapon and International Order* (Yale University Press: 2017), 74–75.

emphasis. We should not conflate the idea that campaigns are cumulative with the idea that their component operations are inherently marginal or small in effect. For example, in delegitimization campaigns to undermine a population's faith in a political or economic institution, a single operation might introduce a societal-wide impact, but that operation, itself, may have benefitted from the knitting together of both pooled and sequenced operations. Much is to be gained analytically by employing the construct of campaign to look for those connections.

Strategic advantage and sources of national power

'Strategic advantage' is a widely used concept, though often left undefined.[32] Strategic advantage for the purposes of this analysis of how and why cyber campaigns maybe used by state and semi-state and non-state actors can be understood as an outcome in which a relative change occurs in the bilateral, regional or global distribution of power in the favour of the actor engaged in the cyber campaign. The distribution of power within the international system, as Alexander Wendt notes, consists of both material and ideational forces and is operationalised across economic, military and, political forms.[33]

Power is notoriously difficult to operationalise. But, this definition of strategic advantage, importantly, moves us away from the narrow understanding of power widely held across the discipline: 'an actor controlling another to do what that other would otherwise not do'.[34] Not least, cyber campaigns can change, what Barnett and Duval call, the 'structural positions of states'. According to the scholars, 'structural power conceive structure as an internal relation-that is, a direct constitutive relation such that the structural position, A, exists only by virtue of its relation to structural position, B'.[35] Cyber campaigns, for example, can turn two initially symmetric relations to asymmetrical relations – and vice versa – due to loss of innovation and productive capacity.

Characteristics of cyberspace

Cyberspace has several structural features that enable actors to operate in ways not possible in the conventional domain(s). Cyberspace is defined as 'a global domain within the information environment comprising the interdependent network of information technology infrastructures and resident

[32]The term can have multiple meanings. For a longer discussion see: Max Smeets, 'The Strategic Promise of Offensive Cyber Operations', *Strategic Studies Quarterly* 12/3 (Fall 2018), 90–113.
[33]Alexander Wendt, *Social Theory of International Politics*, (Cambridge: Cambridge University Press: 1999).
[34]Quoted in: Michael Barnett and Raymond Duval, 'Power in International Politics', *International Organization*, 59/1(2005), 39–75.
[35]Barnett and Duval, 'Power in International Politics', 53.

data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'.[36] Conventional wisdom holds that cyberspace is an interconnected, malleable environment.[37] This means that 'constant contact' is an inherent feature of cyberspace.

Cyberspace's interconnectedness changes the ability of actors to exert influence beyond their own boundaries through the use of capabilities. Projecting power through conventional means is costly, and requires states to overcome a range of logistical challenges.[38] Kenneth Boulding referred to this as the 'loss-of-strength gradient' (LSG); the ability of an actor to deploy military force decreases with geographical distance.[39] Although the internet is still constrained by infrastructure, user demand and government restrictions that create a 'differentiated centrality', unlike conventional forms of hard power, the use of cyber means is hardly mediated by geographical distance.[40] Nor do actors require the same degree of control over the 'global commons' as for conventional force projection.[41] As a result, actors have greater reach and opportunities to conduct and sustain cyber operations and campaigns over a wider range of targets.

There is considerable variation in the resources required to execute different cyber operations.[42] Whilst certain types of operations can only be conducted by a small set of highly resourced actors – due to the knowledge, material and organisational obstacles actors must overcome to prepare and

[36]'Cyberspace Operations', Joint Publication 3–12(R), Department of Defense, (2013); also adopted in Fischerkeller and Harknett, 'Deterrence is Not a Credible Strategy for Cyberspace' For alternative definitions see: U.S. Cyberspace Policy Review; Hannes Ebert and Tim Maurer, 'Contested Cyberspace and Rising Powers', *Third World Quarterly* 34/6 (2013), 1054–74. For a similar definition see: Sami Saydjari, 'Defending Cyberspace', *Computer* 35/12 (2002), 125–27; Lucas Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security* 38/2 (2013), 7–40; Lucas Kello, 'Cyber Disorders: Rivalry and Conflict in a Global Information Age', Presentation, International Security Program Seminar Series, Cambridge, Mass. International Security Program, Belfer Center for Science and International Affairs, Harvard Kennedy School (2012, May). http://www.belfercenter.org/publication/cyber-disorders-rivalry-and-conflict-global-information-age.

[37]For a discussion on importance of malleable (instead of man-made) nature of cyberspace see: Martin Libicki, 'Cyberspace is not a war fighting domain', I/S: A journal of Law and Policy for the Information Society, 8:2, 321–36, 324; For a discussion of the potential limitations of the man-made and malleable notion: See Dorothy E. Denning, 'Rethinking the Cyber Domain and Deterrence', *Joint Force Quarterly* 77 (1 April 2015), http://ndupress.ndu.edu/Publications/Article/581864/rethinking-the-cyber-domain-and-deterrence/

[38]Barry Posen, 'Command of the Commons: The Military Foundation of U.S. Hegemony', *International Security* 28/1 (2003), 5–46.

[39]Kenneth E. Boulding, *Conflict and Defense: A General Theory* (New York: Harper and Brothers 1962), 79, 230–31; for similar statement see: Nicholas J. Spykman, *America's Strategy in World Politics: The United States and the Balance of Power* (New York: Harcourt, Brace 1942), 393–94.

[40]The degree to which geography still plays a role differs per operation. On spatiality in cyberspace also see: Matthew Zook, Lomme Devriendt, and Martin Dodge, 'Cyberspatial Proximity Metrics: Reconceptualizing Distance in the Global Urban System', *Journal of Urban Technology* 18/1 (January 2011), 93–114.

[41]Posen, 'Command of the Commons'.

[42]There remains a lack of scholarship on the logistical factors in cyber operations. For an overview see: Max Smeets and JD Work, 'Operational decision making for cyber operations: In Search of a Model', *Cyber Review* (Forthcoming).

execute these activities – the barriers of entry to conduct other operations are much lower.[43] Hence, a broad group of actors can conduct and sustain some types of cyber operations.

The technological nature of the environment and the inherent dynamic that follows from the technology suggests that the opportunities for seeking initiative is exponentially higher in cyberspace across both time and geographical space.

Incentives to conduct cyber campaigns below the threshold of armed attack

The above discussion does not imply that the 'high-and-right' type of cyber operations cannot occur. Yet, the awareness that cyber activity below the threshold of armed attack can cumulatively have a significant strategic impact raises an important question: why would actors conduct a highly destructive cyber operation if they can obtain a strategic advantage in a less conspicuous manner?[44]

Conducting a mix of smaller operations, instead of a large-scale attack, has a number of advantages. Not least, a 'slow-bleed' strategy is more difficult to discern than a 'quick-stab' approach given the diverse manner and long-time frame in which cyber operations can be linked. Cumulative loss (or gain) could occur without notice and the time separation from actual operations being conducted and being forensically discovered itself can be exploited for advantage.

An additional incentive for activity that is below the threshold of war is that the current state of international law and commonly held expectations about behaviour (norms) remain immature in this arena of competition. This holds for domestic law as well. Cyber operations that can be directed between the seams of domestic authorities and regulations have greater potential for success or at least a higher probability of a lack of effective response. Finally, cyber operations and campaigns conducted below the threshold of war negate the conventional and nuclear superiority that some

[43] On the development requirements of the high-end type of capabilities, see: Rebecca Slayton, 'What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment', *International Security* 41/3 (2016/2017), 72–109; Lindsay, 'Stuxnet and the Limits of Cyber Warfare'; For non-academic discussions on cases other than Stuxnet see: Kaspersky Lab, 'Equation Group: The Crown Creator of Cyber-Espionage', (16 February 2015), https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage; Max Smeets, 'A Matter of Time: On the Transitory Nature of Cyberweapons', *Journal of Strategic Studies* 41/12(2018), 6–32; Yet, the organisational obstacles should equally not be neglected. See: Max Smeets, 'Integrating Offensive Cyber Capabilities; meaning, dilemmas, and assessment', *Defence Studies* 18/4 (2018), 395–410; Max Smeets, 'Organisational Integration of Offensive Cyber Capabilities: A Primer', 2017 9th International Conference on Cyber Conflict (Tallinn: NATO CCD COE Publications: 2017).

[44] For a longer discussion on the meaning of armed attack, especially with the context of United Nations Charter (UN Charter), see: Tom Ruys, *'Armed Attack' and Article 51 of the UN Charter* (Cambridge: Cambridge University Press 2010).

states have over other states, since the form of the operation or campaign does not credibly induce armed military response.[45]

Changing the empirical lens

When we change the theoretical lens and realise that activity below the threshold of armed attack can still be strategically meaningful, how does it change our interpretation of ongoing cyber activity? In this first part of this section, we analyse important state activity through the conventional cyber-war lens. As a crucial case study, we then discuss Chinese cyber operations through the cyber campaigns' lens as an example.

China as the peaceful cyber power?

Various state actors have conducted highly disruptive or destructive cyber operations in the past. The United States has conducted numerous known cyber operations which sought to disrupt, deny, degrade or destroy. The US government has publicly acknowledged 'waging a cyberwar' against the Islamic State (the British government has equally made this claim).[46] Unacknowledged, but prominently discussed, remains the operation the US conducted alongside Israel, called 'Olympic Games', against the Iranian nuclear facilities in Natanz.[47] Some have attributed other disruptive attacks against entities in the Middle-East to the US government as well.[48]

[45]The effectiveness of a deterrence strategy rests on the immediate cost-benefit calculus of a potential attacker. It is a reasonable supposition, however, to explore the idea that given U.S. conventional and military strength states seeking to challenge U.S. relative power would experiment with cyber campaigns that explicitly avoid going near what the United States might consider armed attack. Counterintuitively, it maybe the effectiveness of deterrence of war that is driving so much cyber behaviour below it. See, Michael Fischerkeller, Richard Harknett, and Jelena Vicic, 'The Limits of Deterrence and the Need for Persistence, in Aaron Brantly (forthcoming: 2019).

[46]The success of these operations, however, remains contested – even among the most senior policy-makers. See: Ashton Carter, 'A Lasting Defeat: The Campaign to Destroy ISIS', *Report*, Belfer Center for Science and International Affairs, Harvard Kennedy School (October 2017). https://www.belfercenter.org/LastingDefeat; Max Smeets and Herbert S. Lin, 'Offensive Cyber Capabilities: To What Ends?' 2018 10th International Conference on Cyber Conflict, T. Minárik, R. Jakschis, L. Lindström (Eds.) (NATO CCD COE Publications: Tallinn: 2018), https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2003%20Offensive%20Cyber%20Capabilities.%20To%20What%20Ends.pdf

[47]Sanger, *Confront and Conceal* (New York: Penguin Random House 2013); Lindsay, 'Stuxnet and the Limits of Cyber Warfare'.

[48]In late April 2012, an incident came to light when the *New York Times* published a story that a mysterious malware attack was shutting down computer systems at businesses throughout Iran. References to these wiper attacks were later found in a conversation between General Keith Alexander, then director of the National Security Agency (NSA) and commander of U.S. Cyber Command and Sir Iain Robert Lobban, Director of UK's Government Communications Headquarters (GCHQ). Thomas Erdbrink, 'Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet', *The New York Times*, (23 April 2012), https://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html; NSA, 'Iran – Current Topics, Interaction with GCHQ', (12 April 2013), https://www.eff.org/files/2015/02/21/20150210-intercept-iran_current_topics_-_interactions_with_gchq.pdf

Furthermore, the *New York Times* has built a convincing case that the US has been able to disrupt the missile program of North Korea for a least some time through offensive cyber.[49] North Korean hackers, in turn, are known for wiping out the computer systems of several South Korean financial companies and broadcasters in 2013 and Sony networks in 2014.[50] The May 2017 attack, dubbed WannaCry, was also known to be conducted by the North Korean government. WannaCry struck across the globe encrypting files and demanding users to pay a 300 USD ransom in bitcoins.[51] The ransomware hit more than 200,000 computer systems across the world, with some estimating the total damage exceeding 5 billion USD.[52] If we only consider the 2017–2018 attacks, Russia has equally contributed its fair share of conducting disruptive cyber operations. As if WannaCry did not already cause enough damage and disruption, soon after NotPetya was released by the Russian government. NotPetya used the same exploit and was seeded to initially infect Ukrainian computer systems, though it quickly spread across the world affecting thousands of computers.[53] NotPetya was a wiper in disguise: although it purported to be ransomware like WannaCry, the worm was unable to revert its own changes – leaving

[49]William J. Broad and David E. Sanger, 'U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight', *New York Times*, (4 March 2017), https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defence.html; David E. Sanger and William J. Broad, 'Trump Inherits a Secret Cyberwar against North Korean Missiles', *New York Times* (4 March 2017), https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html; David E. Sanger and William J. Broad, 'Hand of U.S. Leaves North Korea's Missile Program Shaken', *New York Times*, (18 April 2017), https://www.nytimes.com/2017/04/18/world/asia/north-korea-missile-program-sabotage.html; Herbert Lin, 'Hacking a Nation's Missile Development Program', in Herbert Lin and Amy Zegart (eds.), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Brookings Press 2018).

[50]The wiping in the case of Sony networks was considered to be not the main purpose of the attack, but used to wipe traces. For an excellent overview of North Korea's (early) wipers see: Symantec Security Response, 'Destover: Destructive malware has links to attacks on South Korea' (3 December 2014), https://www.symantec.com/connect/blogs/destover-destructive-malware-has-links-attacks-south-korea

[51]Symantec Security Response, 'What you need to know about the WannaCry Ransomware', *Symantec Corporation*, (23 October 2017), https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

[52]The ransomware worm propagated through EternalBlue, was an exploit released by the Shadowbrokers, targeting a vulnerability in an early version of Microsoft's implementation of the Server Message Block, a transport protocol that allows devices to communicate for remote services. As Alex Hern, reported of the Guardian notes, 'Microsoft fixed the EternalBlue weakness in March, before it was released by the Shadow Brokers, tipped off by the NSA that it was likely to be made public. But two months later, many organisations had yet to install the patch'. Alex Hern, 'WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017', *The Guardian*, (30 December 2017), https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware; Also see: Lily Hay Newman, 'The leaked NSA spy tool that hacked the world', *Wired*, (7 March 2018), https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/; On the operational requirements see: Steve Morgan, 'Global Ransomware Damage Costs Predicted To Exceed 5 Billion USD In 2017', *Cybersecurity Ventures*, (18 May 2017), https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/.

[53]Whilst NotPetya's initial victims were in Ukraine, it soon spread more widely hitting various multinationals, including shipping company Maersk and pharmaceutical company Merck. Andy Greenberg, 'The Untold Story of NotPetya, The most devastating cyberattack in history', *Wired*, (22 August 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

damages beyond repair.[54] Over the past decade, the Iranian government has also become active in the cyber domain.[55] In August 2012, a case dubbed 'Shamoon', also known as Disttrack, gained global attention. Shamoon targeted the world's largest oil company, Saudi Aramco. Whilst a group named 'Cutting Sword of Justice' claimed responsibility, there is strong evidence the Iranian government was behind the operation.[56] The malware had a wiper component which served to erase files and a reporter component which meant to send the information about the files back to the attackers. Shamoon led to the destruction of 30,000 workstations.[57] And whilst Shamoon's code contained several coding flaws, private sector reports indicate that Iran has learned from its earlier mistakes considering subsequent activity.[58]

Considering these operations over the past decade, one could argue that China is the most peaceful cyber power in the international system There are few – if any – publicly reported cases in which Chinese government actors have conducted cyber operations against international actors which sought to disrupt, deny, degrade, or destroy.[59] One potential case would be the Chinese government's attack on *GitHub*, a web-based hosting service based in the United States, in March 2018. The attack against GitHub was the biggest distributed denial of service (DDoS) attack recorded to date.[60] Yet, the

[54] Josh Fruhlinger, 'Petya ransomware and NotPetya malware: What you need to know now', CSO (17 October 2017), https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

[55] 'Since the Stuxnet attack', Siboni and Korenfeld write, Iran 'has been working hard to improve its cyberspace defences on the one hand, while building up cyberspace intelligence gathering and offensive capability on the other'. Gabi Siboni and Sami Kronenfeld, 'Iran and Cyberspace warfare', *Military and Strategic Affairs* 4/3 (2012), 101–17.

[56] Lucian Constantin, 'Kill timer found in Shamoon malware suggests possible connection to Saudi Aramco attack', *Computerworld* (23 August 2012), http://www.computerworld.com/article/2491501/malware-vulnerabilities/kill-timer-found-in-shamoon-malware-suggests-possible-connection-to-saudi-ar.html

[57] It did not cause physical damage to the production facilities of the oil company. The payload overwrites the segment of a hard drive responsible for rebooting the system as well as the partition table and most files with random data, including a small segment of an image that allegedly shows a burning American flag. See: Symantec Security Response, 'The Shamoon Attacks', *Symantec Official Blog*, (16 August 2012), http://www.symantec.com/connect/blogs/shamoon-attacks; also see: Bill Trivitt, 'The Evolution of APTs (Advanced Persistent Threats)', *Information System Security Association*, http://kern.issa.org/wp-content/uploads/2013/08/The-Evolution-of-APTsv1_2.pdf, p. 9.

[58] Kaspersky Lab, 'From Shamoon to Stonedrill: Wipers attacking Saudi organizations and beyond',(2017), https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf

[59] For a discussion on potentially earlier cases see: Jon Lindsay, 'The Impact of China on Cybersecurity: Fiction and Friction', *International Security* 39/3 (2014/2015), 7–47.

[60] Whilst GitHub officials states that the attackers used a range of new techniques to create this flood of traffic, this type of DDoS attack (known as amplification attack) has been conducted before. Dan Goodin from Ars Technica previously reported on this technique in 2014 when it was used to take down servers for several online gaming services. See: Dan Goodin, 'DoS attacks that took down big game sites abused Web's time-sync protocol', *Ars Technica*, (2014, 8 January), https://arstechnica.com/information-technology/2014/01/dos-attacks-that-took-down-big-game-sites-abused-webs-time-synch-protocol/; On GitHub response see: Robert K. Knake, 'Placing the Office of Personnel Management Hack in Perspective', (15 June 2015), *Council on Foreign Relations*, https://www.cfr.org/blog/placing-office-personnel-management-hack-perspective.

motivation of this attack was primarily *domestic* censorship.[61] The attack specifically targeted pages for two Github users that circumvent China's firewall: the *GreatFire* and the Chinese mirror site of the *New York Times*.[62] The Chinese government also likely carried out a Distributed Denial of Service (DDoS) against independent media sites in Hong Kong during the Umbrella Movement in 2014.[63]

China certainly has the capacity to conduct CNA-like operations. Since 2002, after the 16th Party Congress, the People Liberation Army (PLA) has sought to integrate effectively information warfare into its military doctrine to leapfrog development.[64] China, like Russia, does not use the term 'cyber', and instead uses the more holistic term 'information security'.[65] One of the main terms used by China in the early 2000s was INEW – integrated network electronic warfare (wangdian yiti zhan).[66] We know from military exercises that the country has performed cyber activities that, in US intelligence parlance, would be described as CNA. According to a report from *Northrop Grumman*, during an exercise in the Beijing Military Region in mid-2004, the Red Force' conducted cyber operations to disrupt the C2 information systems of the 'Blue Force'.[67] Another exercise is known to have taken place in 2009 by the People's Liberation Army (PLA) in the Lanzhou Military Region, of which CNA was also a part.[68]

China is only the most 'peaceful' cyber power if we consider cyber activity in narrow terms of cyberwar; that is violence and sudden disruption of the international system. Such a conceptual framing misses the fact that China *is*

[61] Also, the range of activity dedicated to the Great Firewall could be understood in this way; as a disruption through filtering of information flow and functionality that if a western government engaged in would be regarded as illegal denial of access to data/information.

[62] Paul Mozur, 'China Appears to Attack GitHub by Diverting Web Traffic', *The New York Times*, (30 March 2015), https://www.nytimes.com/2015/03/31/technology/china-appears-to-attack-github-by-diverting-web-traffic.html

[63] Party Olson, 'The Largest Cyber Attack in History has been hitting Hong Kong Sites', *Forbes*, (20 November 2014) https://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/#dc0017b38f6e

[64] As Inkster notes, 'Chinese military strategy combines IW and electronic warfare into the single concept of wangdian yitizhan (Integrated Network Electronic Warfare)'; Nigel Inkster, 'China's Cyber Power' *Adelphi Series*, (2016, May), p. 99; Chinese understanding of information warfare is said to be inspired by US writing on the 'revolution in military affairs'. See: Andrew F. Krepinevich, (ed.), *The Military-Technical Revolution: A Preliminary Assessment* (Washington, D.C.: Center for Strategic and Budgetary Assessments, Office of Net Assessment 2002).

[65] Ibid; also see Lindsay, 'The Impact of China on Cybersecurity'.

[66] Kevin Pollpeter, 'Chinese Writings on Cyberwarfare and Coercion', in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford University Press 2015).

[67] Yet, the references the report of Northrop Grumman uses are PLA propaganda, which means that it is hard to tell if the PLA even conducted these operations or if it was white carded. Bryan Krekel, George Bakos, Christopher Barnett, 'the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation', Prepared for The US-China Economic and Security Review Commission, Northrop Grumman Corporation (2009).

[68] Zoe Li, 'What we know about the Chinese army's alleged cyber spying unit, ' *CNN* (20 May 2014), http://edition.cnn.com/2014/05/20/world/asia/china-unit-61398/index.html

an incredibly active, strategically motivated actor in this space that is able to change the balance of power in the international system through offensive cyber operations. As former Director of National Intelligence Admiral McConnel argues, 'Rather than destroying US competitiveness through "cyberwar," [Chinese actors] are exploiting our systems for information advantage – looking for the characteristics of a weapon system by a defense contractor or academic research on plasma physics, for example – not in order to destroy data and do damage'.[69] Shifting our lens from the conflict of cyberwar to the strategic competition of cyber campaigns, reveals a very different picture of Chinese cyber behaviour.

Uncovering Chinese cyber activity as campaigns

Senior Western officials have repeatedly claimed that China conducts cyber-espionage operations on a 'massive scale'.[70] Compared to traditional espionage, cyber espionage is 'easier, happens at a much greater pace, and proceeds a great haul'.[71] A group of threat intelligence researchers started a database in 2015 on '[Advanced Persistent Threat (APT)] Groups and Operations' aggregating existing private sector reports.[72] It currently lists 79 APTs operating from China.[73] Some of these actors are known to have an enormous range. In 2011, Dmitri Alperovitch, then at McAfee, published a report on a set of targeted attacks against at least 70 governments and organisations spanning over several years.[74] The group behind these attacks is frequently attributed to the Shanghai-based Chinese Army Signals Intelligence branch, Unit 61,398 (ie. 2nd Bureau of the People's Liberation Army General Staff 3rd Department.)[75] Whilst the title of the report is 'Operation Shady RAT', the activity might be better described as a *series* of operations – relying on similar tactics, techniques and procedures (at least between 2006 and 2010/2011) – connecting to different campaigns. As

[69]Nathan Gardels, 'MIke McConnell: An American Spymaster on Cyberwar', Huffpost (8 August 2009), https://www.huffingtonpost.com/nathan-gardels/mike-mcconnell-an-america_b_227944.html

[70]See: Bruce Sterling, 'E-spionage' (12 April 2008), *Wired*, https://www.wired.com/2008/04/e-spionage/; It is hard to provide a precise estimate of the cumulative costs of Chinese cyber operations to Western society – even if we just consider *industrial* espionage activities alone. Estimates range from a few billion dollars a year to over hundreds of billions a dollars a year.

[71]Adam Segal, *Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs 2016).

[72]Pasquale Stirparo, David Bizeul, Brian Bell, Ziv Chang, Joel Esler, Kristopher Bleich, Maite Moreno, Monnappa K A J. Capmany, Paul Hutchinson, Boris Ivanov, Andre Gironda, Devon Ackerman, Carlos Fragoso, Eyal Sela, Florian Egloff, 'APT Groups and Operations', https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1864660085

[73]Ibid; Segal notes that there are approximately twenty Chinese cyber-espionage units that 'go after political and military intelligence, as well as that will bolster China's economic competitiveness'. Segal, *Hacked World Order*.

[74]Dmitri Alperovitch, 'Revealed: Operation Shady RAT', McAfee, http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf

[75]The group is also known as TG-8223, APT 1, Brownfox, Group 3, Shanghai Group or Comment Crew.

Alperovitch notes, a 'fascinating aspect that the logs have revealed to us is the changing tasking orders of the perpetrators as the years have gone by'.[76] Whereas most of the early activity was focused on industrial espionage, an increasing number of later operations also sought to achieve other goals.[77]

The US government only started to publicly acknowledge systematic Chinese data exfiltration in August 2006, after the Chinese actors had successfully intruded Non-classified Internet Protocol (IP) Router Network (NIPRNet), the Department of Defense's network for exchanging 'sensitive but unclassified' information, and downloaded up to 20 terabytes of data.[78] Most of the private sector reporting on Chinese cyber operations started to be published around the same time. Yet, Chinese cyber-espionage operations are known to go back since at least the early 2000s.[79] And they are certainly expected to go ahead far in the future. Several reports suggest that China has taken the gloves off in recent years and ramped up its (industrial) espionage.[80]

Some experts remain sceptical about the strategic impact of Chinese activity below the threshold of armed attack. The bulk of the criticism comes in two forms. First, some argue that the actors conducting these operations are 'China-based' or 'Chinese-speaking', but not related to the Chinese government. The hacker community in China indeed existed *before* the government started to double-down on offensive cyber operations in the late 1990s.[81] Scott Henderson, an analyst who worked in the US intelligence community as a Chinese linguist for two decades, indicates that the origin of Chinese hacking (or better termed 'cracking') date back to 1994 when the internet was made available to a (certain section) of the population.[82] The hacking community grew in the years after following the formation of several non-state groups such as the Green Army and the China Eagle Union in 1997.[83]

[76] Alperovitch, 'Revealed', p. 6.
[77] For a detailed overview see *Ibid* p.7–13.
[78] James C. Mulvenon, 'Chinese cyber espionage', *Testimony Before the Congressional-Executive Commission on China* (25 June 2013), https://www.cecc.gov/sites/chinacommission.house.gov/files/CECC%20Hearing%20-%20Chinese%20Hacking%20-%20James%20Mulvenon%20Written%20Statement.pdf.
[79] For example, Kaspersky's first known sample of 'Nettraveler' goes back to 2004. Nettraveler is still active today. Kaspersky Lab, 'APT Logbook', https://apt.securelist.com/#!/threats/.
[80] On 25 September 2015. President Barack Obama and Chinese President Xi Jin Ping agreed that neither government would 'conduct or knowingly support cyber-enabled theft of intellectual property' for economic an economic advantage. Editorial Board, 'The U.S. must take action to stop Chinese industrial espionage', *The Washington Post*, (4 November 2018), https://www.washingtonpost.com/opinions/the-us-must-take-action-to-stop-chinese-industrial-espionage/2018/11/04/66ccd5a6-ded2-11e8-b3f0-62607289efee_story.html?noredirect=on&utm_term=.b34bf6a75420.
[81] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, (Cambridge: Cambridge University Press: 2018).
[82] Scott J. Henderson, *The Dark Visitor: Inside the World of Chinese Hackers* (2007).
[83] As Henderson notes: 'The Green Army was founded by a Shanghai hacker going by the online name of Goodwill, it was reported to have had a membership of around 3,000 people from Shanghai, Beijing, and Shijiazhuang. [. . .] The group disbanded in 2000 and its rise and fall was described as "confusing" by insiders who consider it one of the enduring symbols of the Chinese hacker movement'. Ibid.

Also, for several Chinese threat actors – e.g. Hurricane Panda, Goblin Panda, Night Dragon, IceFog, Dust Storm, Dragon OK, SVCMONDR and SabPub group – most reports from cybersecurity firms only indicate it is a 'China-based actor' or an actor with Chinese-origin.[84] In other cases, only general patterns of behaviour are reported about the threat actor from which state responsibility is extrapolated.[85] For example, FireEye writes about threat actor Naikon: '[s]uch a sustained, planned development effort, coupled with the group's regional target and mission, lead us to believe that this activity is state sponsored – mostly likely by the Chinese government'.[86] That means that we should indeed be careful of describing all activity to the Chinese state.[87]

Yet, over the years the non-state and state activity has become increasingly 'interlinked' as the government is tightening its control.[88] FireEye has also revealed with a 'high level of confidence' that there is a 'Digital Quartermaster' which supports several advanced actors in China.[89] The quartermaster supplies malware and maintains command and control infrastructure used in distinct but overlapping campaigns since at least 2013.[90]

Furthermore, we *do* have a high level of certainty that some of the most active groups are (directly connected to) the government – especially based on evidence published in recent years.[91] For example, Crowdstrike and others

[84]For an overview of reports see Stirparo et al., 'APT Groups and Operations'.

[85]On Pitty Tiger, *Airbus* writes the threat actor 'is probably not a state-sponsored group of attackers. They lack the experience and financial support that one would expect from state-sponsored attackers. We suppose this group is opportunistic and sells its services to probable competitors of their targets in the private sector'. Graham Cluley, 'Targeted Trident cyber-attack against defence company', *Naked Security*, (2010, June), https://nakedsecurity.sophos.com/2010/06/24/targeted-trident-cyberattack-defence-company/; Airbus, 'The Eye of the Tiger', (2014, 11 July), http://blog.airbuscybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2.

[86]The unit is likely backed or part of PLA unit 78020. FireEye, 'APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation', (2015), https://www.fireeye.com/blog/threat-research/2015/04/apt_30_and_the_mecha.html; Kurt Baumgartner and Maxim Golovkin, 'The Naikon APT', SecureList (14 May 2015), https://securelist.com/the-naikon-apt/69953/

[87]Similar to Naikon, for the following threat actors most reports only state that it is 'Chinese origin' or 'Chinese based': Lotus Blossom (only a report from Palo Alto Networks is more detailed), APT 6 (likely government), Emissary Panda, Hellsing (likely criminal), Anchor Panda (like government based on target base), Covert Grove, Scarlet Mimic Group (likely government as it targets Uyghur activists), C0d0so (likely government, considering techniques according to iSight), Mofang (likely government based on target base, according to FoxIT), Shiqiang Gang (unlikely state). For links to all reports see: Stirparo et al., 'APT Groups and Operations'.

[88]On the monopolisation of cyber force in China see: Maurer, Cyber Mercenaries, p. 115–19; On the 'centralization of the cyber mission', see John Costello, 'Statement on China's Intelligence Services and Espionage Operations', before the U.S.-China Economic and Security Review Commission', (9 June 2016), https://www.uscc.gov/sites/default/files/transcripts/June%2009%2C%202016%20Hearing%20Transcript.pdf p. 17; William C. Hannas, James Mulvenon, and Anna B. Puglisi, 'Chinese Industrial Espionage: Technology Acquisition and Military Modernization', *Asian Security Studies* (2013).

[89]FireEye, 'Supply Chain Analysis: From Quartermaster to Sunshop', (2014)

[90]Ibid.

[91]There are different 'levels' of attribution, and equally a 'spectrum of responsibility' of states for cyber attacks. See: Herbert Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts', *Journal of International Affairs*, The Cyber Issue (2016, Winter); Jason Healey, 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks', Issue Brief The Atlantic Council, (2012), https://www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf.

have been able to track various espionage activity directly back to Unit 61486, the 12th Bureau of the PLA's General Staff Department 3rd Department headquartered in Shanghai. Also, the activity of cyber-espionage group known as UPS could initially not be traced back to the Chinese government (in part because of little overlap across their operations).[92] Yet, later analysis directly connected UPS' activity to the Chinese Ministry of State Security (MSS) with a high degree of confidence.[93] Finally, Alperovitch's study, discussed above, has not been the only report on activity coming from inside PLA's Unit 61398.[94]

Second, some scholars argue that the Chinese government might be able to acquire all this information but is unable to turn it into a competitive advantage.[95] According to Jon Lindsay, '[a]lthough Western cyber defenders can observe the exfiltration of petabytes of data to Chinese servers, they cannot so readily measure China's ability to use the data'.[96] The scholar continues to note that 'China faces major challenges in converting foreign inputs into innovative output given the notoriously compartmentalised and hierarchical nature of Chinese bureaucracy, underdeveloped high-end equipment manufacturing capacity, and chronic dependence on foreign technology and know-how'.[97] Mauro Gilli and Andrea Gilli in a recent *International Security* article focus on the ease to imitate the United States' advanced weapon systems.[98] Using China's efforts to copy U.S. stealth fighters in a comparative case study, their argument is that military systems have become so complex it is hard for second-tier states to catch up.

While the barrier to comparative advantage may not be low, we must maintain a long-term perspective – instead of single case view – with respect to Chinese campaigns. As Robert Farley suggests, 'We can grant that China is some 20 years behind the United States in terms of developing stealth

[92]Erica Eng and Dan Caselden, 'Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign', FireEye (23 June 2015), https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html; Counter Threat Unit Research Team, 'Threat Group-0110 Targets Manufacturing and Financial Organizations Via Phishing', Secureworks (25 July 2014), https://www.secureworks.com/blog/threat-group-0110-targets-manufacturing-and-financial-organisations-via-phishing; Symantec Security Response, 'Buckeye cyberespionage group shifts gaze from US to Hong Kong' (6 September 2016), https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

[93]Intrusion Truth, 'APT3 is Boyusec, a Chinese Intelligence Contractor' (9 May 2017), https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/

[94]A detailed analysis of all Chinese actors is beyond the scope of this paper. For equally compelling attribution evidence about state responsibility of Chinese cyber operations see reports on Shell Crew, Maverick Panda, the Beijing Group, and IXESHE.

[95]For an excellent discussion on the phases of adoption see: Tai Ming Cheung, *Fortifying China: The Struggle to Build a Modern Defense Economy* (Ithaca, NY: Cornell UP 2009).

[96]Jon R. Lindsay, 'The Impact of China on Cybersecurity: Fiction and Friction', *International Security* 39/3 (2014/15), 7–47, 24.

[97]Ibid, p. 25.

[98]Andrea Gilli and Mauro Gilli, 'Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage', *International Security* 43/3 (2019), 141–89.

technology, and that the most advanced of China's stealth projects (including the J-20 and the J-31) have significant problems. But China is also ahead of … every country in the world not named the United States in stealth technology and has accomplished this despite starting from a lower core of industrial competencies than Europe, Japan, or Russia. And China has succeeded in part because of its legitimate access to the global technology market, in part because of its theft of key technologies, and in part because of high state investment to develop core industrial competencies'.[99]

Gilli and Gilli's work can easily be misunderstood. Their analysis does not suggest that China did not gain anything out of the cyber-enabled IP-theft in the case of the F-35. Instead, the scholars note that in light of the massive amount of data China accessed, they gained relatively little out of it.[100] One gain, for example, concerns the frontal radar reduction of the Chinese fighter, shortening the range at which it can be detected (and hence, extending the range of potential operation).[101] Furthermore, not all IP and technology that China steals is as complex as military technology systems. Indeed, Gilli and Gilli's research findings are limited to *military* technology. Also, even the *possible* use of stolen information is significant as target actors need to divert significant time and energy evaluating and adjusting to possible consequences. In the case of the F-35, Lockheed Martin had to rewrite parts of the software to vulnerable systems and redesign specialised communications and antenna arrays for the stealth aircraft. In a tightening competition between leading states, the gaining of initiative and the necessitating of resource diversion, if cumulated, can lead to sustainable advantage.

Furthermore, the transfer of technology is only *one* of the goals sought by China through cyber campaigns.[102] In 2014, Chinese hackers stole almost 22 million records of current and former government employees as part of the Office of Personnel Management (OPM) breach.[103] Stolen data included

[99]For an excellent critical analysis of the article see: Robert Farley, 'Is China's Path to Military Parity With the US Through Intellectual Property Theft Doomed?', *The Diplomat*, (8 March 2019), https://thediplomat.com/2019/03/is-chinas-path-to-military-parity-with-the-us-through-intellectual-property-theft-doomed/; Robert Farley, 'From the Dreadnought to Modern Stealth: Seeking Military Technological Superiority', *The Diplomat*, (11 March 2019), https://thediplomat.com/2019/03/from-the-dreadnought-to-modern-stealth-seeking-military-technological-superiority/; Robert Farley, 'Intellectual Property, Defense Technology, and the Future of Great Power Relations', *The Diplomat*, (14 March 2019), https://thediplomat.com/2019/03/intellectual-property-defence-technology-and-the-future-of-great-power-relations/.

[100]We thank Mauro Gilli for clarifying this point.

[101]Also, despite purported challenges in flight success, it is the case that China is attempting certain direct technology imitations in that the fuselage of China's new fifth-generation jet fighter, the Shenyang FC-31 (or J-31), looks remarkably similar to that of the F-35 (Joint Strike Fighter) and F-22. US Pacific Command's Admiral Samuel Locklear half-jokingly told a reporter that 'Chinese military equipment looks surprising similar to American weapons'.

[102]When talking about a 'contested cyberspace', Lindsay only assesses to what degree 'Chinese cyber espionage is systematically eroding the competitiveness of Western firms'. Lindsay, The Impact of China on Cybersecurity, p. 12.

[103]The OPM hack was only discovered and disclosed a year later.

names, dates, places of birth, security background checks, data on intelligence and military personnel, and the fingerprint data of 5.6 million employees. The hackers even accessed the Standard Form 86 which includes information 'perfect for blackmail', such as records of drug use, alcohol addiction and financial problems.[104] This information could be combined with medical data stolen from Anthem Insurance, travels records from United Airlines, and hotel reservation data from the Marriott International to create a more complete picture of US personnel and importantly their movement.[105] As Costello argues in more detail at U.S. Congressional hearing: 'most chillingly, China will marry its database of federal and military workers with real-time intelligence collected from other sources. While the OPM data [. . .] isn't live; it can't change and grow and respond to military operations and policy and policymaking–it does provide a perfect targeting set for follow-on exploitation and a natural framework in which to correlate and evaluate new intelligence. And that is most likely how it will be used in the future'[106]

In fact, applying the construct of cyber campaign to link each one of these individual breaches creates a distinctive analytical conclusion than treating them as isolated thefts of private sector and government data. Reporting at the time suggested that the information gathered could be used for counter-intelligence reasons to track possible Chinese individuals who might be meeting with Americans with security clearances. Whether correct or not as a specific explanation of this case, using the concept of cyber campaigns allows the linkage between a breach of an American government agency and exfiltration of a hotel chain data to be explored as a significant capacity to affect overall US and Chinese intelligence-gathering capabilities to compete effectively against each other.[107]

Finally, even if the barrier to direct imitation of technology is high, it is not at all clear that imitation is the main objective. Using the technology-information transfer to understand the parameters of US high-tech military capability can be leveraged to make determinations on how to design around or overwhelm it. The comparative advantage comes indirectly and perhaps through

[104]Adam Segal, 'How China is preparing for cyberwar', *The Christian Science Monitor*, (20 March 2017), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar

[105]'This is not the end of American human intelligence', said Joel Brenner, former senior counsel at the National Security Agency, 'but it's a significant blow'. Nicole Perlroth, Amie Tsang and Adam Satariano, 'Marriott Hacking Exposes Data of Up to 500 Million Guests', *The New York Times*, (30 November 2018), https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html; David Perera and Joseph Marks, 'Newly disclosed hack got 'crown jewels'', *Politico* (2015, 12 June), https://www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954.

[106]John Costello, 'Panel I: Structure, Reforms, and Capabilities of Chinese Intelligence Services', U.S. – China Economic and Security Review Commission (9 June 2016), https://www.uscc.gov/sites/default/files/transcripts/June%2009,%202016%20Hearing%20Transcript.pdf.

[107]This potential counter-intelligence linkage is discussed in David Sanger et.al., 'Marriott Data Breach is Traced to Chinese Hackers as US Readies Crackdown on Beijing', *New York Times*, (11 December 2018), https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

reliance on less sophisticated scaled swarming technology that overwhelms the most advanced weaponry – modern-day English long-bowman to the French cavalry at Agincourt.[108]

Limitations and objections: Old wine in a new bottle?

The preceding sections have advanced a number of claims about the current state of the field and potential of cyber campaigns. This section takes up a possible objection to the arguments put forward in this article. One may agree with our assessment of the limitations of the current literature as well as the opportunities cyberspace enables, but argue that this is old wine in a new bottle: it is all part of an aged-old intelligence game.[109]

Rovner argues that '[t]he cyberspace competition is an intelligence contest in a technologically novel domain'.[110] The scholar continues to argue 'Looking through the intelligence lens puts the cyberspace competition in perspective, but it requires a willingness to live with ambiguity'.[111] In similar vein, Gartzke and Lindsay argue that 'computer network operations should mainly be understood as *expanding the scope* of intelligence and covert operations [emphasis added]' and, since the use of deception is self-limiting, 'cyber warfare … is best understood as low-intensity conflict behavior … rather than as a separate form of strategic warfare'.[112] Additionally, Lindsay argues that the political effects of such behaviours are ambiguous, again, because of the constraints of conspiracy.[113] Thus, though cyberspace facilitates expanding the scope of covert operations, the resulting effects merely represent a difference in degree (an increased count) because independent effects across an expanded scope are still ambiguous or marginal due to the burdens of deception.

[108]Bret Stephens, The U.S.Military; like the French at Agincourt?', *New York Times*, (25 April 2019), https://www.nytimes.com/2019/04/25/opinion/us-military.html.

[109]The extent to which this notion of intelligence competition instead of overlaps with our statement of cyber campaigns partially depends on the definition one employs of intelligence. As Wheaton and Beerbower note in a prominent essay, 'nowhere is there a single-agreed upon definition of intelligence. The intelligence community, quite literally, does not know what it is doing. [U.S. government legal amendments] make a circular journal though a forest of legislative language to arrive, in the end, precisely where it began: "intelligence is information". […] The law-enforcement intelligence community is somewhat better off, but just barely'. In this discussion, we decided to focus on the more expansive conceptions of intelligence contest as these are expected to be most similar to our notion of strategic campaigns. Kristan J. Wheaton and Michael T. Beerbower, 'Towards a New Definition of Intelligence', *Stanford Law & Policy Review* 17/2 (April 2006), 319–20, 324, 327.

[110]Rovner argues that an 'intelligence contest' has five elements: i) information collection, ii) information exploitation; iii) covert undermining of moral, institutions, and alliances; iv) sabotage; and v) the prepositing of assets for intelligence collection in the event of a conflict. Joshua Rovner, 'Cyber War as an Intelligence Contest', War on the Rocks (16 September 2019), https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

[111]Ibid.

[112]Erik Gartzke and John R. Lindsay, 'Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace', op. cit.

[113]Jon R. Lindsay, 'Cyber Espionage', op. cit.

However, Michael Warner argues that, where formerly covert operations' influence was at 'the margins of state practice', that may now be changing because cyberspace allows states to execute covert operations *at scale*.[114] The ability to execute continuous, cyber campaigns at scale, he argues, allows for individual, marginal effects to aggregate into the class of strategic effects. Thus, whereas covert operations have historically been a secret, supplemental factor in international relations, Warner argues that cyberspace facilitates their functioning through scale as a secret, independent factor.[115] Indeed, the empirical record makes clear that an expansion in scope of operations has been accompanied by an expansion in scale and, when taken together, is resulting in a *difference in kind* and not merely degree.[116]

How do scope and scale of cyber operations relate to strategic significance? We could effectively adopt Gartke's criteria, although by dropping the confusing term cyberwarfare.[117] To paraphrase, in order for cyber operations to be relevant in 'grand strategic terms' (or 'pivotal in world affairs'), they would have to 'accomplish tasks typically associated with terrestrial military violence'.[118] These include deterring or compelling, i.e., generating influence through the prospect of damage or loss, maintaining or altering the balance of power, and resisting or imposing disputed outcomes. We can leave off much of that and agree that that cyber operations do not serve well as coercive instruments. However, the empirical record supports an argument that cyber campaigns and operations can be pivotal in world affairs by independently (absent coupling with conventional capabilities) supporting the maintenance or alteration of the balance of power and resisting disputed outcomes. Indeed, cyberspace has created opportunities for states to realise such strategic aims *without having to resort to military violence*. A different game is afoot.

[114]Michael Warner, 'A Matter of Trust: Covert Action Reconsidered', *Studies in Intelligence* 63/4, 33–41.
[115]Ibid.
[116]Indeed, concerns regarding 'scale' played an important role in elevating the importance of cyberspace in United States Department of Defense. In 2011, Deputy Defense Secretary William Lynn III announced that 'as the scale of cyberwarfare's threat' to U.S. national security and the U.S. economy has come into view 'the Pentagon has formally recognized cyberspace as a new domain of warfare' and that 'recognizing that the scale of the effort to protect cyberspace had outgrown the military's existing structures, Defense Secretary Robert Gates ordered the consolidation of the task forces into a single four-star command, the U.S. Cyber Command, which began operations in May 2010 as part of the U.S. Strategic Command'. These concerns with scale proved prescient, as nearly every annual Director of National Intelligence threat assessment report since references year-over-year increases in scope and scale of adversary operations affecting U.S. national interests (and the same can be found in private-sector threat reports). William J. Lynn III, 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs* 5 (2010), 13; Dennis C. Blair, Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence, 2 February 2010, https://www.dni.gov/files/documents/Newsroom/Testimonies/20100202_testimony.pdf, and Daniel R. Coats, Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community, 13 February 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA—Unclassified-SSCI.pdf; For an example of private sector reporting, see FireEye's M-Trends reports.
[117]Gartzke, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth'.
[118]We note there might be disagreement on this point between scholars arguing that cyberspace is an intelligence contest. Ibid.

Conclusion

The argument of this article is that we should study cyber means not as enablers of war, although they can be, but more critically as the strategic alternative to it. To this end, we have introduced the prospect that cyber operations below the threshold of war can impact national sources of power and thus have a strategic impact on the distribution of power. This notion stands in contrast to the premise which underlies much of the cyber literature: that only highly disruptive or destructive cyberattacks can achieve strategic advantage (and for many authors that is unlikely to occur).

The analytical reorientation to broaden from the cyberwar construct to cyber strategic competition through cyber campaigns matters a great deal for policy. The argument implies that cyberspace introduces new ways and means of degrading national power by attaining strategic impact through continuous campaigns comprised of often-covert, less violent cyber operations with cumulative effects has not dominated most western countries cyber strategies over the past twenty years.[119] Because cyberspace is a new dimension through which relative power can be strategically challenged without resort to armed conflict, states must re-think their policy to effectively protect sources of national power. The emergence of nuclear weapons created a whole new approach to strategic thinking summed up famously by Bernard Brodie who concluded, that 'thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them'.[120] Both operational and campaign behaviour in cyberspace appears to be pushing us towards a similar critical pivot in security thinking. While war maybe averted, strategic loss and gain may still occur. This potentiality is backed empirically – states are active in cyber campaigns.

Getting the right framework to understand these core dynamics is essential. Ultimately, this paper is arguing for an opening of the aperture in the study of cybersecurity studies. How cyber means enable war-fighting and how they could impact militarised crises and escalation are important avenues for further research.[121] But an equally important new avenue is research that starts with the premise that strategic cyber competition could be pursued with the same intent and overall objective traditionally associated with war, but achieve those ends through other means.

[119]The shift in 2017–9 in US strategy documents aligns with the construct introduced in this paper. See Richard J. Harknett, 'United States Cyber Command's New Vision: What it Entails and Why it is Important', *Lawfare* (March 2018). https://lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters

[120]The quote and its' significance is discussed in detail in Richard Harknett, 'State Preferences, Systemic Constraints, and the Absolute Weapon', in TV Paul, James Wirtz, and Richard Harknett, *The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order* (Ann Arbor: Univ. of Michigan Press 1998), 47.

[121]For an excellent recent study see: Austin Carson, *Secret Wars: Covert Conflict in International Politics*, (Princeton: Princeton University Press: 2018) Carson's theory explicitly links the decision to operate covertly with decisions to limited war dynamics the desire for escalation control. See Chapter 1, 2, and 3.

Acknowledgements

For written comments on early drafts, we would like to thank Michael Fischerkeller, Mauro Gilli, Jelena Vicic, Diana van der Watt and two anonymous reviewers.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Dr. Richard J. Harknett is Professor and Head of the Department of Political Science at the University of Cincinnati, Co-director of the Ohio Cyber Range Institute, and Chair of the Center for Cyber Strategy and Policy. He served as an inaugural Fulbright Scholar in Cyber Studies at Oxford University and as the inaugural Scholar-in-Residence at US Cyber Command and the National Security Agency, where he assisted at the Command in examining strategic approaches to cyberspace. He was consulted, along with others in government and academia, in the drafting of core strategic and operational concepts associated with persistent engagement as well as cyber legislation in Congress.

Dr. Max Smeets is a senior researcher at the Center for Security Studies (CSS). He is also an Affiliate at Stanford University Center for International Security and Cooperation and Research Associate at the Center for Technology and Global Affairs, University of Oxford.

Bibliography

Airbus, 'The Eye of the Tiger', 11 Jul. 2014. http://blog.airbuscybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2

Alperovitch, Dmitri, 'Revealed: Operation Shady RAT', *McAfee*. http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf

Arquilla, John, 'Rebuttal Cyberwar Is Already Upon Us', *Foreign Policy*, Mar/Apr 2012. 192; ProQuest pp. 84 doi:10.1094/PDIS-11-11-0999-PDN.

Arquilla, John and David Ronfeldt, 'Cyberwar Is Coming!' *Comparative Strategy* 12/2 (1993), 141–65. doi:10.1080/01495939308402915.

Arquilla, John and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica: Rand Corporation 2001).

Arquilla, John and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: The Rand Corporation 1997).

Barnett, Micael and Raymond Duval, 'Power in International Politics', *International Organization* 59/1 (2005), 39–75. doi:10.1017/S0020818305050010.

Baumgartner, Kurt and Maxim Golovkin, 'The Naikon APT', *SecureList*, 14 May 2015. https://securelist.com/the-naikon-apt/69953/

Bendrath, Ralf, 'The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection', *Information & Security* 7 (2001), 80–103.

Bendrath, Ralf, 'The American Cyber-angst and the Real World - Any Link?', Paper presented at: International Studies Association Annual Convention, University of Bremen, Montreal, QC, 2004

Betz, David J. and Tim Stevens, 'Cyberspace and the State: Towards a Strategy for Cyber-Power', *Adelphi Series* 51/424 (2011), 75–98. doi:10.1080/19445571.2011.636956.
Blair, Dennis C., 'Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence', 2 Feb. 2010. https://www.dni.gov/files/documents/Newsroom/Testimonies/20100202_testimony.pdf
Borghard, Erica D. and Shawn W. Lonegran, 'The Logic of Coercion in Cyberspace', *Security Studies* 26/3 (2017), 452–81. doi:10.1080/09636412.2017.1306396.
Boulding, Kenneth, E, *Conflict and Defense: A General Theory* (New York: Harper and Brothers 1962), 79, 230–231.
Broad, Willaim J. and David E. Sanger, 'U.S. strategy to Hobble North Korea was Hidden in plain sight', *New York Times*, 4 Mar. 2017. https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defense.html
Carson, Austin, *Secret Wars: Covert Conflict in International Politics* (Princeton: Princeton University Press 2018).
Carter, Ashton, 'A Lasting Defeat: The Campaign to Destroy ISIS', Report, Oct. (Belfer Center for Science and International Affairs, Harvard Kennedy School 2017). https://www.belfercenter.org/LastingDefeat
Cavelty, Myriam Dunn, *Cyber-Security and Threat Politics US Efforts to Secure in the Information Age* (Abingdon: Routledge 2008).
CBS News, 'Stuxnet: Computer worm opens new era of warfare', *60 Minutes*,4 Mar. 2012. doi:10.1094/PDIS-11-11-0999-PDN.
Cheung, Tai Ming, *Fortifying China: The Struggle to Build a Modern Defense Economy* (Ithaca, NY: Cornell UP 2009).
Clarke, Richard A. and Robert K. Knake, *Cyber War* (New York: Ecco 2010).
Cluley, Graham, 'Targeted trident cyber-attack against defence company', *Naked Security*, Jun.. https://nakedsecurity.sophos.com/2010/06/24/targeted-trident-cyber attack-defence-company/
Coats, Daniel R., 'Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community Feb. 13, 2018. https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA—Unclassified-SSCI.pdf
Collins, Sean and Stephen McCombie, 'Stuxnet: The Emergence of a New Cyber Weapon and Its Implications', *Journal of Policing, Intelligence, and Counter Terrorism* 7/1 (2012), 80–91. doi:10.1080/18335330.2012.653198.
Constantin, Lucian, 'Kill Timer found in Shamoon Malware suggests possible connection to Saudi Aramco Attack', *Computerworld*, 23 Aug. 2012. http://www.computerworld.com/article/2491501/malware-vulnerabilities/kill-timer-found-in-shamoon-malware-suggests-possible-connection-to-saudi-ar.html
Costello, John, 'Panel I: Structure, Reforms, and Capabilities of Chinese Intelligence Services', U.S. –China Economic and Security Review Commission, 9 Jun. 2016. https://www.uscc.gov/sites/default/files/transcripts/June%2009,%202016%20Hearing%20Transcript.pdf
Costello, John, 'Statement on China's Intelligence Services and Espionage Operations,' before the U.S.-China Economic and Security Review Commission', 9 Jun. 2016. https://www.uscc.gov/sites/default/files/transcripts/June%2009%2C%202016%20Hearing%20Transcript.pdf
Counter Threat Unit Research Team, 'Threat Group-0110 Targets Manufacturing and Financial Organizations via Phishing', *Secureworks*, 25 Jul. 2014. https://www.secureworks.com/blog/threat-group-0110-targets-manufacturing-and-financial-organizations-via-phishing
Department of Defense, 'Cyberspace Operations', Joint Publication 3-12(R), Feb. (2013)

Deibert, Ronald J., 'Cyclone in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War', *Security Dialogue* 43 (2012), 3–24. doi:10.1177/0967010611431079.

Denning, Dorothy E., 'Stuxnet: What Has Changed?', *Future Internet* 4 (2012), 672–87. doi:10.3390/fi4030672.

Denning, Dorothy E., 'Rethinking the Cyber Domain and Deterrence', *Joint Force Quarterly*, 1 Apr. 2015, pp. 77. http://ndupress.ndu.edu/Publications/Article/581864/rethinking-the-cyber-domain-and-deterrence/

Editorial Board, 'The U.S. must take action to stop Chinese Industrial Espionage', *The Washington Post*, 4 Nov. 2018. https://www.washingtonpost.com/opinions/the-us-must-take-action-to-stop-chinese-industrial-espionage/2018/11/04/66ccd5a6-ded2-11e8-b3f0-62607289efee_story.html?noredirect=on&utm_term=.b34bf6a75420

Eneken, Tikk, Kadri Kaska and Liis Vihul, 'International Cyber Incidents: Estonia 2007', (Tallinn: NATO CCDCOE 2010) 14–25, 33; in Ottis eds., 'Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective', Proceedings of the 7th European Conference on Information Warfare and Security (Plymouth: Academic Publishing Limited 2008).

Eng, Erica and Dan Caselden, 'Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign', *FireEye*, 23 Jun. 2015. https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

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

Farley, Robert, 'From the dreadnought to modern stealth: Seeking military technological superiority', *The Diplomat*, 11 Mar. 2019. https://thediplomat.com/2019/03/from-the-dreadnought-to-modern-stealth-seeking-military-technological-superiority/

Farley, Robert, 'Intellectual property, defense technology, and the future of great power relations', *The Diplomat*, 14 Mar. 2019. https://thediplomat.com/2019/03/intellectual-property-defense-technology-and-the-future-of-great-power-relations/

Farley, Robert, 'Is China's path to military parity with the US through intellectual property theft doomed?', *The Diplomat*, 8 Mar. 2019. https://thediplomat.com/2019/03/is-chinas-path-to-military-parity-with-the-us-through-intellectual-property-theft-doomed/

Farwell, James P. and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War', *Survival: Global Politics and Strategy* 53/1 (2011), 23–40. doi:10.1080/00396338.2011.555586.

FireEye, 'Supply Chain Analysis: From Quartermaster to Sunshop', 2014. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-malware-supply-chain.pdf

FireEye, 'APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation', 2015. https://www.fireeye.com/blog/threat-research/2015/04/apt_30_and_the_mecha.html

Florian Egloff, 'Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates', DPhil Thesis, University of Oxford, 2018

Fruhlinger, Josh, 'Petya Ransomware and NotPetya Malware: What You Need to Know Now', *CSO*, 17 Oct. 2017. https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

Gabi, Siboni and Sami Kronenfeld, 'Iran and Cyberspace Warfare', *Military and Strategic Affairs* 4/3 (2012), 101–17.

Gardels, Nathan, 'Mike McConnell: An American Spymaster on Cyberwar', *Huffpost*, 8 Aug. 2009. https://www.huffingtonpost.com/nathan-gardels/mike-mcconnell-an-america_b_227944.html

Gartzke, Erik, 'The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth', *International Security* 38/2 (2013), 41–73. doi:10.1162/ISEC_a_00136.

Gilli, Andrea and Mauro Gilli, 'Why China Has Not Caught up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage', *International Security* 43/3 (2019), 141–89. doi:10.1162/isec_a_00337.

Goodin, Dan, 'DoS Attacks that Took down Big Game Sites Abused Web's Time-sync Protocol', *Ars Technica*, 8 Jan. 2014. https://arstechnica.com/information-technology/2014/01/dos-attacks-that-took-down-big-game-sites-abused-webs-time-synch-protocol/

Greenberg, Andy, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 Aug. 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Gross, Michael Joseph, 'A declaration of cyber-war', *Vanity Fair*, Apr. 2011.

Guerrero-Saade, Juan Andres, Costin Raiu, Daniel Moore and Thomas Rid, 'Penquin's Moonlit Maze: The Dawn of Nation-State Digital Espionage', Kaspersky Lab, 2018. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf

Hannas, Wiliam C., James Mulvenon and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* Asian Security Studies (Abingdon: Routledge 2013).

Harknett, Richard., 'State Preferences, Systemic Constraints, and the Absolute Weapon', in TV Paul, James Wirtz and Richard Harknett (eds.), *The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order* (Ann Arbor: Univ. of Michigan Press 1998), 47–72.

Harknett, Richard, 'Review of Brandon Valeriano, Benjamin M. Jensen, Ryan C. Maness, Cyber Strategy: The Evolving Character of Power and Coercion' *H-Net Reviews in Social Science*, Oct. 2018, pp. 1–3

Harknett, Richard J., 'United States Cyber Command's New Vision: What It Entails and Why It Is Important', *Lawfare*, Mar. 2018. https://lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters

Hayden, Michael, *Playing the Edge: American Intelligence in the Age of Terror* (New York City: Penguin Random House 2016).

Healey, Jason., 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks', *Issue Brief The Atlantic Council*, 2012. https://www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf

Healey, Jason and Karl Grindal, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington DC: Cyber Conflict Studies Association 2013).

Henderson, Scott J., *The Dark Visitor: Inside the World of Chinese Hackers* (FortLeavenworth, KS: Foreign Military Studies Office 2007).

Hern, Alex., 'WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017', *The Guardian*, 30 Dec. 2017. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

Hollis, David M., 'Cyberwar Case Study: Georgia 2008', *Small Wars Journal* (6 January 2011), 1–10. https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Inkster, Nigel, 'China's cyber power', *Adelphi Series*, May 2016.

Intrusion Truth, 'APT3 Is Boyusec, a Chinese Intelligence Contractor', 9 May 2017. https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/

Junio, Timothy J., 'How Probable Is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate', *Journal of Strategic Studies* 36/1 (2013), 125–33. doi:10.1080/01402390.2012.739561.

Kaspersky Lab, 'Equation Group: The Crown Creator of Cyber-Espionage', 16 Feb. 2015. https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage

Kaspersky Lab, 'From Shamoon to Stonedrill: Wipers Attacking Saudi Organizations and Beyond', 2017. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf

Kaspersky Lab, 'APT Logbook'. https://apt.securelist.com/#!/threats/

Kello, Lucas, 'Cyber Disorders: Rivalry and Conflict in a Global Information Age', Presentation, International Security Program Seminar Series, Cambridge, Mass. International Security Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2012. http://www.belfercenter.org/publication/cyber-disorders-rivalry-and-conflict-global-information-age

Kello, Lucas, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security* 38/2 (2013), 7–40. doi:10.1162/ISEC_a_00138.

Kello, Lucas, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press 2017).

Knake, Robert K. 'Placing the Office of Personnel Management Hack in Perspective', *Council on Foreign Relations*, 15 Jun. 2015. https://www.cfr.org/blog/placing-office-personnel-management-hack-perspective

Krekel, Bryan, George Bakos and Christopher Barnett, 'The Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation', Prepared for The US-China Economic and Security Review Commission, Northrop Grumman Corporation (2009).

Krepinevich, Andrew F., ed., *The Military-Technical Revolution: A Preliminary Assessment* (Washington, D.C.: Center for Strategic and Budgetary Assessments, Office of Net Assessment 2002).

Langner, Ralph., 'Stuxnet: Dissecting a Cyberwarfare Weapon', *Security and Privacy* 9/3 (2011), 49–51. doi:10.1109/MSP.2011.67.

Li, Zoe, 'What We Know about the Chinese Army's Alleged Cyber Spying Unit', *CNN*, 20 May 2014. http://edition.cnn.com/2014/05/20/world/asia/china-unit-61398/index.html

Libicki, Martin, *Cyberwar and Cyberdeterrence* (Santa Monica: RAND Corporation 2009). https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Libicki, Martin C., 'Cyberspace Is Not a Warfighting Domain' *I/S A Journal of Law and Policy for the Information Society* 8/2 (2012), 325–40. http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf.

Liff, Adam P., 'Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War', *Journal of Strategic Studies* 35/3 (2012), 401–28. doi:10.1080/01402390.2012.663252.

Liff, Adam P., 'The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio', *Journal of Strategic Studies*, 134–38.

Lin, Herbert, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts', *Journal of International Affairs* 70/1 (Winter 2016), 75–138.

Lin, Herbert, 'Hacking a Nation's Missile Development Program', in Herbert Lin and Amy Zegart (eds.), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Brookings Press 2018), 151–172.

Lindsay, Jon, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* 22/3 (2013), 365–404. doi:10.1080/09636412.2013.816122.

Lindsay, Jon, 'The Impact of China on Cybersecurity: Fiction and Friction', *International Security* 39/3 (2014/2015), 7–47. doi:10.1162/ISEC_a_00189.

Lindsay, Jon. R., 'The Impact of China on Cybersecurity: Fiction and Friction', *International Security* 39/3 (2014/2015), 7–47. doi:10.1162/ISEC_a_00189.

Lynn, William J, III, 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs* 89/5 (September/October 2010), 97–108.

Lynn, William J, III, 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs* 89/5 (2010), 13.

Mahnken, Thomas G., 'Cyber War and Cyber Warfare'', in Kristin Lord and Travis Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. 2 (Washington DC: CNAS 2011), 53–62.

Matthew., Zook, Lomme Devriendt and Martin Dodge, 'Cyberspatial Proximity Metrics: Reconceptualizing Distance in the Global Urban System', *Journal of Urban Technology* 18/1 (January 2011), 93–114. doi:10.1080/10630732.2011.578411.

Maurer, Tim, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press 2018).

McConnell, Mike., 'Cyberwar Is the New Atomic Age', *New Perspectives Quarterly* 26/3 (Summer 2009). doi:10.1111/j.1540-5842.2009.01103.x.

McGraw, Gary, 'Cyber War Is Inevitable (Unless We Build Security In)', *Journal of Strategic Studies* 36/1 (2013), 109–19. doi:10.1080/01402390.2012.742013.

Michael, Fischerkeller, Richard Harknett and Jelena Vicic, 'The Limits of Deterrence and the Need for Persistence, in Aaron Brantly', (forthcoming: 2019)

Monte, Matthew, *Network Attacks and Exploitation: A Framework* (Indianapolis: Wiley 2015).

Morgan, Steve, 'Global Ransomware Damage Costs Predicted To Exceed $5 Billion In 2017', *Cybersecurity Ventures*, 18 May 2017. https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

Mozur, Paul, 'China Appears to Attack GitHub by Diverting Web Traffic', *The New York Times*, 30 Mar. 2015. https://www.nytimes.com/2015/03/31/technology/china-appears-to-attack-github-by-diverting-web-traffic.html

Mulvenon, James C., 'Chinese Cyber Espionage', *Testimony Before the Congressional-Executive Commission on China*, 25 Jun. 2013. https://www.cecc.gov/sites/chinacommission.house.gov/files/CECC%20Hearing%20-%20Chinese%20Hacking%20-%20James%20Mulvenon%20Written%20Statement.pdf

Newman, Lily Hay, 'The Leaked NSA Spy Tool that Hacked the World', *Wired*, 7 Mar. 2018. https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/

Nissenbaum, Helen., 'Where Computer Security Meets National Security', *Ethics and Information Technology* 7/2 (2005), 61–73. doi:10.1007/s10676-005-4582-3.
NSA, 'Iran - Current Topics, Interaction with GCHQ', 12 Apr. 2013. https://www.eff.org/files/2015/02/21/20150210-intercept-iran_current_topics_-_interactions_with_gchq.pdf
Olson, Party, 'The Largest Cyber Attack in History Has Been Hitting Hong Kong Sites', *Forbes*, 20 Nov. 2014. https://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/#dc0017b38f6e
Panetta, Leon E., 'Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City', *News Manuscript U.S Department of Defense*, Oct. 2012. http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136
Paulo, Shakarian, 'The 2008 Russian cyber campaign against Georgia', *Military Review*, Nov.–Dec., 2011, p. 63–64 doi:10.1016/j.tvjl.2010.05.029.
Perera, David and Joseph Marks., 'Newly Disclosed Hack Got 'Crown Jewels'', *Politico*, 12 Jun. 2015. https://www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954
Perlroth, Nicole., Amie Tsang and Adam Satariano., 'Marriott Hacking Exposes Data of up to 500 Million Guests', *The New York Times*, 30 Nov. 2018. https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html
Pollpeter, Kevin, 'Chinese Writings on Cyberwarfare and Coercion', in Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford University Press 2015), 138–162.
Posen, Barry, 'Command of the Commons: The Military Foundation of U.S. Hegemony', *International Security* 28/1 (2003), 5–46. doi:10.1162/016228803322427965.
President's Commission on Critical Infrastructures, 'Infrastructure Protection, Critical Foundations: Protecting America's: The Report of the President's Commission on Critical Infrastructure Protection', 13 Oct. 1997. https://www.fas.org/sgp/library/pccip.pdf
Rid, Thomas, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35/1 (2012), 5–32. doi:10.1080/01402390.2011.608939.
Rid, Thomas., 'Think Again: Cyberwar', *Foreign Policy*, 27 Feb. 2012. http://foreignpolicy.com/2012/02/27/think-again-cyberwar
Rid, Thomas, *Cyber War Will Not Take Place* (Oxford: Oxford University Press 2013).
Rid, Thomas, 'Is Cyberwar Real?' in response to Jarno Limnéll Foreign Affairs', Mar./Apr.
Rovner, Joshua., 'Cyber War as an Intelligence Contest', *War on the Rocks*, 16 Sept. 2019. https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/
Ruys, Tom, *'Armed Attack' and Article 51 of the UN Charter* (Cambridge: Cambridge University Press 2010).
Sanger, David, 'Marriott Data Breach Is Traced to Chinese Hackers as US Readies Crackdown on Beijing', *New York Times*, 11 Dec. 2018. https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html
Sanger, David. E., *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown 2012).
Sanger, David. E and William J. Board, 'Hand of U.S. Leaves North Korea's Missile Program Shaken', *New York Times*, 18 Apr. 2017. https://www.nytimes.com/2017/04/18/world/asia/north-korea-missile-program-sabotage.html

Sanger, David. E and William J. Broad., 'Trump Inherits a Secret Cyberwar against North Korean Missiles', *New York Times*, 4 Mar. 2017. https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html

Saydjari, Sami, 'Defending Cyberspace', *Computer* 35/12 (2002), 125–27. doi:10.1109/MC.2002.1106187.

Scott, James and Drew Spaniel., 'China Espionage Dynasty: Economic Death by A Thousand Cuts', *Institute for Critical Infrastructure Technology*, 28 Jul. 2016. http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.07.28.China_Espionage_Dynasty/ICIT-Brief-China-Espionage-Dynasty.pdf

Segal, Adam, *Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs 2016).

Segal, Adam, 'How China Is Preparing for Cyberwar', *The Christian Science Monitor*, 20 Mar. 2017. https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar

Slayton, Rebecca, 'What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment', *International Security* 41/3 (2016/2017), 72–109. doi:10.1162/ISEC_a_00267.

Smeets, Max, 'Organisational Integration of Offensive Cyber Capabilities: A Primer', 2017 9th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, 2017.

Smeets, Max, 'A Matter of Time: On the Transitory Nature of Cyberweapons', *Journal of Strategic Studies* 41–12 (2018), 6–32. doi:10.1080/01402390.2017.1288107.

Smeets, Max, 'The Strategic Promise of Offensive Cyber Operations', *Strategic Studies Quarterly* 12/3 (Fall 2018), 90–113.

Smeets, Max, 'Integrating Offensive Cyber Capabilities; Meaning, Dilemmas, and Assessment', *Defence Studies* 18/4 (2018), 395–410. doi:10.1080/14702436.2018.1508349.

Smeets, Max and Herbert S. Lin, 'Offensive Cyber Capabilities: To What Ends?'in T. Minárik, R. Jakschisand L. Lindström (eds.), 2018 10th International Conference on Cyber Conflict (Tallinn: NATO CCD COE Publications 2018). https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2003%20Offensive%20Cyber%20Capabilities.%20To%20What%20Ends.pdf

Smeets, Max and JD Work, 'Operational Decision Making for Cyber Operations: In Search of a Model', *Cyber Defense Review* (Forthcoming).

Spykman, Nicholas J., *America's Strategy in World Politics: The United States and the Balance of Power* (New York: Harcourt, Brace 1942), 393–94.

Stephens, Bret. 'The U.S.Military; like the French at Agincourt?' *New York Times*, 25 Apr. 2019. https://www.nytimes.com/2019/04/25/opinion/us-military.html

Sterling, Bruce, 'E-spionage', *Wired*, 12 Apr. 2008. https://www.wired.com/2008/04/e-spionage/

Stirparo, Pasquale, David Bizeul, Brian Bell, Ziv Chang, Joel Esler, Kristopher Bleich, Maite Moreno, K A J. Monnappa, Paul Hutchinson Capmany, Boris Ivanov, Andre Gironda, Devon Ackerman, Carlos Fragoso, Eyal Sela and Florian Egloff, 'APT Groups and Operations'. https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1864660085

Stone, John, 'Cyber War Will Take Place!', *Journal of Strategic Studies* 36/1 (2013), 101–08. doi:10.1080/01402390.2012.730485.

Symantec Security Response, 'The Shamoon Attacks', *Symantec Official Blog*, 16 Aug. 2012. http://www.symantec.com/connect/blogs/shamoon-attacks

Symantec Security Response, 'Destover: Destructive Malware Has Links to Attacks on South Korea', 3 Dec. 2014). https://www.symantec.com/connect/blogs/destover-destructive-malware-has-links-attacks-south-korea

Symantec Security Response, 'Buckeye Cyberespionage Group Shifts Gaze from US to Hong Kong', 6 Sept. 2016. https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

Symantec Security Response, 'What You Need to Know about the WannaCry Ransomware', *Symantec Corporation*, 23 Oct. 2017. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

Tikk, Eneken, Kadri Kaska, and Liis Vihul, *Cyber Attacks Against Georgia* (Tallinn: NATO CCDCOE 2008).

Trivitt, Bill, 'The Evolution of APTs (Advanced Persistent Threats), 'Information System Security Association. http://kern.issa.org/wp-content/uploads/2013/08/The-Evolution-of-APTsv12.pdf

U.S. Cyberspace Policy Review, Ebert, Hannes and Tim Maurer, 'Contested Cyberspace and Rising Powers', *Third World Quarterly* 34/6 (2013), 1054–74. doi:10.1080/01436597.2013.802502.

Valeriano, Brandon and Ryan C. Maness, 'The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11', *Journal of Peace Research* 51/3 (2014), 347–60. doi:10.1177/0022343313518940.

Valeriano, Brandon and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press 2015).

Warner, Michael, 'A Matter of Trust: Covert Action Reconsidered', *Studies in Intelligence* 63/4 (2019), 33–41.

Wendt, Alexander, *Social Theory of International Politics* (Cambridge: Cambridge University Press 1999).

Wheaton, Kristan J. and Michael T. Beerbower, 'Towards a New Definition of Intelligence', *Stanford Law & Policy Review* 17/2 (April 2006), 319–20.

The White House, 'The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive', *White Paper*, 22 May 1998, pp. 63. www.fas.org/irp/offdocs/paper598.h

Yould, Rachel, 'Beyond the American Fortress: Understanding Homeland Security in the Information Age', in Robert Latham (ed.), *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security* (New York, NY: The New Press 2003).

Zetter, Kim, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Penguin Random House 2014).

Zetter, Kim, 'New Evidence Links a 20-Year-Old Hack on the US Government to a Modern Attack Group', *Motherboard*, 3 Apr. 2017. https://motherboard.vice.com/en_us/article/vvk83b/moonlight-maze-turla-link