Article details

Boeke, S., Broeders & D. (2018), The Demilitarisation of Cyber Conflict, Survival 60(6): 73-90.
Doi: 10.1080/00396338.2018.1542804

Routledge
Taylor & Francis Group

Survival

Global Politics and Strategy

ISSN: 0039-6338 (Print) 1468-2699 (Online) Journal homepage: https://www.tandfonline.com/loi/tsur20

The Demilitarisation of Cyber Conflict

Sergei Boeke & Dennis Broeders

To cite this article: Sergei Boeke & Dennis Broeders (2018) The Demilitarisation of Cyber Conflict, Survival, 60:6, 73-90, DOI: 10.1080/00396338.2018.1542804

To link to this article: https://doi.org/10.1080/00396338.2018.1542804

The Demilitarisation of Cyber Conflict

Sergei Boeke and Dennis Broeders

Speculation over cyber war has moved beyond its initial poles of doomsday and dismissal.[1] Some argued that 'cybergeddon' or a digital Pearl Harbor was looming, others that cyber war had never occurred and probably never would.[2] The front line of the debate has since shifted to whether or not cyberspace has become militarised,[3] if deterrence is possible in cyberspace,[4] and, if the security dilemma applies, how it can be mitigated.[5] In strategic studies, the debate focuses on whether cyber conflict reaches Clausewitzean thresholds of violence and damage.[6] Legal scholars – for example through the Tallinn process – are attempting to define when cyber operations reach the level of an 'armed attack' and 'the use of force', triggering conventional legal reasoning under the framework of the Law of Armed Conflict.[7] While states have agreed – some with regret – that international law applies in the digital world as it does in the offline one, there is no agreement on how.[8] The last round of the United Nations Group of Governmental Experts failed to provide a consensus report in 2017, stalling the process to establish norms of responsible state behaviour in cyberspace.[9] Both the academic debate on cyber conflict and the international policy process to agree to 'rules of the road' are nonetheless built on the same premise: that cyber operations fall under the normative and legal frameworks regulating military conduct during war and peace.

Sergei Boeke is a researcher at the Institute of Security and Global Affairs (ISGA) at Leiden University. **Dennis Broeders** is an associate professor and senior fellow in The Hague Program for Cyber Norms at the ISGA.

Survival | vol. 60 no. 6 | December 2018–January 2019 | pp. 73–90 DOI 10.1080/00396338.2018.1542804

There are, however, good reasons to believe that the frameworks presumed applicable to cyber conflict are actually a bad fit. Two developments support the thesis that the militarisation of cyberspace may actually be the result of a *demilitarisation* of cyber conflict, as the main actors in cyber conflict are not actually military actors. Both the dominant role of foreign-intelligence and security agencies (as opposed to military actors) in cyber operations, and the use of proxies (either private contractors or other non-state actors) in cyber conflict, illustrate that, in practice, cyber conflict largely takes place outside the parameters of international humanitarian law. Other principles of international law still apply to interventions by intelligence services and proxies below the threshold of armed conflict. International law writ large is silent on espionage, but not on covert paramilitary actions or clandestine intelligence activities with disruptive effects. Many states use proxies precisely to render their potentially illegal actions deniable.[10] Nevertheless, if state practice, both directly and indirectly, indicates that there are non-military actors and legal gaps in the cyber domain, the international debate about state behaviour in cyberspace may at least partially be set in the wrong legal key.

Demilitarising cyber conflict?

In the security domain, traditional boundaries between military and civilian, and internal and external security, have long been blurring. The process has been especially intense in the cyber dimension. Lene Hansen and Helen Nissenbaum note that the internet has a tendency to blur classical distinctions deemed crucial to international relations and security studies: those 'between individual and collective security, between public authorities and private institutions, and between economic and political–military security'.[11] Some boundaries fade through technological developments or deliberate policy choices. The latter range from mitigating the problem of scarce resources, such as a shortage of cyber-security professionals, to the desire of state actors to operate with a degree of deniability. Two fundamental boundaries in particular determine under which normative and legal framework cyber operations should fall: the boundary between military operations and foreign-intelligence – that is, espionage – activities, and that between state and private actors in cyber operations.

Intelligence and security agencies vs the military

'Cyberspace operations, because of their nature, may be harder to pigeonhole within the range of military operations', write Gary D. Brown and Andrew O. Metcalf.[12] This may turn out to be an understatement, especially when foreign-intelligence operations are contrasted with regular military operations. Foreign-intelligence actors are primarily concerned with extracting information, and building and maintaining an information position within the enemy's networks (the long game). They face only national constraints on what is considered a legitimate and legal target. The dominant mode of operations is clandestine, such that the activities as well as the perpetrator must remain secret. By contrast, military operations are ultimately overt and are meant to display and use force against an enemy. These two models may meet in the middle in the form of covert action, in which the effects of the operation are visible to the adversary (and potentially the rest of the world), but the hand behind it is not. This creates room for plausible deniability, implausible deniability or at least confusion.[13] To be sure, international law applies regardless of whether intentional interference in the internal affairs of another sovereign state is conducted by military or intelligence services. State action is state action; it is simply tougher to prove in certain non-military cases. In such cases, however, the law is much harder to enforce. In effect, therefore, the legal regime for clandestine and covert operations is murky at best and most firmly grounded in national rather than international law.[14] This indeterminacy is intentional: states are reluctant to specify precisely how they instruct their intelligence officers to break other countries' laws.

Many of the most significant cyber attacks discovered so far are the suspected work of foreign-intelligence and security agencies rather than military actors. Thomas Rid surmised in 2012 that all the then-known politically motivated cyber attacks were merely versions of sabotage, espionage and subversion – and therefore did not amount to cyber war.[15] His observation can be taken one step further: in times of peace, these activities are conducted by intelligence agencies. The fact that some of these agencies, like the US National Security Agency (NSA), have some form of military signature or embedding does not mean that they necessarily operate under

the legal regime for military operations. Even those that are an integral part of the military operate under the legal regime for foreign intelligence. Other countries, like the United Kingdom and Germany, have chosen to embed their foreign-espionage and cyber capacity in purely civilian agencies – Government Communications Headquarters (GCHQ) and the Federal Intelligence Service (BND), respectively.

There is a long and growing list of cyber operations, some labelled as specific Advanced Persistent Threats (APTs) by various cyber-security companies, that can be attributed to different intelligence services.[16] Stuxnet, sometimes heralded as the one cyber attack that reached the level of war,[17] has convincingly been ascribed to the US and Israel by cyber-security companies and investigative journalists (most notably, David Sanger of the *New York Times*).[18] The code was written by the NSA in cooperation with Israel's Unit 8200, but was unleashed – at least on behalf of the US – through the Central Intelligence Agency (CIA). In 2014, the UK's GCHQ was found responsible for a targeted attack on the Belgian telecommunications provider Belgacom, a rare documented case of one NATO ally running a sophisticated cyber-espionage operation on another.[19] In 2017 the virus NotPetya struck several targets in Ukraine, but the collateral damage to other companies worldwide amounted to $10 billion.[20] A coalition of countries attributed the attack to the Russian Federation, and more specifically to the GRU, Russia's military-intelligence agency.[21] In short, foreign-intelligence agencies, and not the regular military, are leading the charge in what is frequently mislabelled cyber war.

For both offence and defence there is a fundamental tension between intelligence collection and military (or policy) action. By their very nature, intelligence agencies lean towards keeping, expanding and deepening the information they possess, avoiding the temptation to use the intelligence and thereby lose the source. The classic example is the extreme secrecy surrounding the Allies' breaking of the Enigma cipher during the Second World War, precluding the operational use of the acquired intelligence in several instances. From a defensive perspective, the intelligence agency's reflex to protect sources inhibits the process of attribution, especially the release of evidence to support a public accusation. In attributing the Sony Pictures

hack to North Korea in 2014 – the first public attribution of a cyber attack to another state – US officials omitted any evidence to back up the claim. Subsequently, officials acknowledged that the NSA had assets present in North Korean networks, and that they could not have provided evidence without compromising sources and methods.[22] Nearly four years later, the FBI indicted a North Korean hacker who was working for North Korea's main intelligence agency on the Sony hack and several subsequent cyber attacks, such as the WannaCry virus.[23] For offence, the same forces are at play. In describing the military effort against the Islamic State (ISIS), Ash Carter, the former US secretary of defense, has expressed his disappointment with US Cyber Command, stating that they never really produced effective cyber weapons or techniques. When they did produce something useful, he added, 'the intelligence community tended to delay or try to prevent its use, claiming cyber operations would hinder intelligence collection'.[24] In cyber operations, then, having your cake and eating it is generally not an option.[25]

'Don't get caught' is the rule

Most importantly, military operations and foreign-intelligence activities operate on the basis of different legal paradigms. Warfare has been subject to international law since Hugo Grotius published his seminal work on the laws of war and peace in 1625. Now International Human Rights Law, the UN Charter and the legal texts grouped under the Law of Armed Conflict regulate state behaviour during armed conflict, building on principles such as proportionality and distinction. By contrast, foreign-intelligence collection has not been regulated by international law, with limits provided by an undefined 'gentlemen's agreement'.[26] The international norm allowing peacetime espionage is partially built on the 1927 SS *Lotus* case by the Permanent Court of International Justice, which articulated an oft-cited principle in international law, essentially permitting everything that is not explicitly prohibited.[27] This leaves 'don't get caught' as the prime informal rule and 'everybody does it' as the first line of defence when one does get caught.

Most liberal democracies have legislated restrictions on how their foreign intelligence can operate abroad, but other regimes are less legalistic and

give their agencies free rein. The use of force by intelligence agencies is a more complicated, and under-discussed, legal field. In essence, the nature of the targeted network already partly indicates whether the attacker's motive is espionage or sabotage. The networks of political parties and government departments are considered legitimate targets for foreign espionage; this generates political and strategic intelligence. Breaching the networks of critical infrastructure such as the electric grid, however, generates no political intelligence. It does, however, provide crucial intelligence for sabotage in times of conflict – but also in peace. During armed conflict, critical infrastructure can be a legitimate target according to the laws of war, but this does not legitimise 'preparation of the battlefield' in an intrusive way. Passive reconnaissance using signals intelligence (SIGINT), human intelligence (HUMINT) or imagery intelligence is accepted as part of the game. But actively hacking targets and leaving implants in the adversary's networks seem as illegitimate as laying remotely controlled sea-mines inside a port in peacetime. In doing so, the agencies step outside their own legal paradigm. Given the nature of cyber operations, more of these transgressions can be expected in the future. The use of covert action is not explicitly covered by international law, though constraints against it are implied in state-to-state rules such as the prohibition against the violation of sovereignty and territorial integrity, and the principle of non-intervention.[28] Any physical destruction rising to the level of an armed attack, however, would be subject to the Law of Armed Conflict.

How to apply recognised international laws in a new domain like cyberspace is subject to much debate. Most cyber operations fall well below the threshold of an 'armed attack' – which would trigger the Law of Armed Conflict – and are executed by foreign-intelligence agencies. Does that mean they are all espionage operations, and thus not explicitly regulated by international law? This question will become increasingly problematic as cyber operations proliferate. Strategic ambiguity may benefit the powerful, but this advantage diminishes in relative value as others join the playing field. Furthermore, the debate about the nature of cyber weapons – including whether that is even an appropriate and useful term – has important legal dimensions. Both the procurement and

the use of a weapon are tied to legal rules and restrictions under domestic (military) law, so labelling something as a weapon has far-reaching legal, policy and political implications.[29]

It may make more sense to describe cyber weapons simply as operations, characterised by what Max Smeets calls their 'transitory nature'.[30] Cyber operations are tailor-made combinations of intelligence, intrusion and attack, and it is seldom clear where one phase ends and another begins. Moreover, the substance of the weapon is software code. This must be adapted and customised to evolving and unforeseen circumstances in the target's network and the overall development of the operation. A cyber weapon is therefore very different from, say, a tank, and it is an open question whether it should be subject to the same military rules with regard to procurement and operational use. Applying the rules – which would include reviewing all changes to the 'weapon' – might grind cyber operations to a halt. Not applying them would effectively keep all cyber operations under the label of foreign-intelligence operations.[31] Neither appears an attractive option in the long run.

Proxies vs state actors

Foreign-intelligence services and military actors may operate under different legal regimes, but they are at least recognised state actors. The Westphalian state system legitimises sovereign states as the security actors in the international domain, formally excluding non-state actors. Even though the monopoly on the legitimate use of force – for both Weberian internal sovereignty as well as Westphalian external sovereignty – is still a relatively new element of modern state formation, its symbolic power cannot be underestimated.[32] While developments such as failed states, international terrorism and private military companies have put cracks in this ideal vision of international security, this monopoly remains a fundamental basis of modern state power and legitimacy. As such, it underpins the international legal order. But actual malicious activities in cyberspace do challenge that standard. Across the board, non-state actors are involved in cyber operations, often in some formal or informal relationship with state actors. Such actors also vary in terms of political legitimacy.

Tim Maurer presents different models of the relationship between states and the proxies they use for cyber operations, based on the degree to which the state actually controls the actors conducting cyber operations on its behalf.[33] He identifies three main proxy relationships: delegation, orchestration and sanctioning.[34] In the first model, the state exerts the most direct control over the proxy; the last consists of only passive support, or even just the turning of a blind eye to their activities. As to legitimacy, there are various political models of the legitimate soldier that at the edges transgress into models that cover illegitimate combatants, such as vigilante forces and mercenaries. (These concepts are captured in Table 1.) Elke Krahmann identifies three types of legitimate combatants: the citizen soldier, embedded in political republicanism; the professional soldier, embedded in republicanism and liberalism; and the private military contractor. The latter is legitimate up to the point where he or she does not engage in actual combat, the preserve of states.[35] The citizen soldier runs the risk of turning into a vigilante, the private military contractor into a mercenary; both are considered unlawful combatants under international law.

Typology of legitimate and illegitimate combatants

The potential blurring of the various models of legitimacy and effective state control is obvious in the case of kinetic operations undertaken by non-uniformed combatants. In cyberspace, where operations are as a rule covert, the provenance of the actor, the nature of the activity and the guiding intent can all remain unclear. Unlike the capabilities of tanks, frigates and combat aircraft, a state's cyber capability is difficult to assess, and not easy to quantify or compare. It is clear, however, that the United States, Israel, China and Russia are the 'top tier' cyber powers. But each sports a different model. The United States combines the professional-soldier model with a heavy reliance on private contractors and private military companies. Israel combines

Table 1. **Types of combatants**

Vigilante	Citizen soldier	Professional soldier	Private military company	Mercenary
Illegal	Legal	Legal	Legal	Illegal
No democratic legitimacy	Republican democratic legitimacy	Mixed republican and liberal democratic legitimacy	Neoliberal legitimacy (contractual and private law)	No democratic legitimacy

the model of the citizen soldier with a heavy reliance on its cyber-security industry, as well as a revolving door between its military and that industry. China employs a hybrid model of the professional soldier and citizen soldier with elements of vigilantism. And Russia combines a model of the professional soldier with vigilante proxies.

In the United States, relations between the military and the defence contractors that cater to its needs have been close since the Second World War. This military–industrial complex has, in turn, given rise to an emerging cyber–military complex.[36] It consists of traditional defence contractors, now possessing cyber-security divisions, and a growing market of start-ups and boutique firms that conduct work substantially but not exclusively for the military.[37] Both the procurement of weapons from private industry and the outsourcing of certain non-combatant tasks to private military companies are considered legal and legitimate. In cyberspace, however, state security agencies are increasingly *contracting in* private cyber-security services and expertise instead of *sourcing out* tasks and product development. This modality results in public–private hybrids that operate behind the closed doors of security and intelligence agencies and the military. In cyber operations, especially where physical effects are generated, it has become increasingly difficult to define the 'tip of the spear'. In the traditional framework of the Law of Armed Conflict, this has implications for the combatants' rights and obligations.[38]

Some legal scholars have argued that the nature of cyber weapons challenges the idea that one can separate the triggermen from others involved in the process. The complex nature of cyber weapons leads 'states to use contractors with technical expertise to constantly modify the features of a weapon in order to overcome the defence of the target, thus blurring the line between the traditional civilian task of weapons development and the traditional combatant task of weapons use'.[39] The *Tallinn Manual*, a non-binding but influential document, argues that 'any civilian fighting in a cyberwar loses legal protections as a civilian'.[40] From an international-law perspective, this suggests that private contractors may shift into the category of mercenary when the effect of an operation transcends a certain level of force and damage. The large number of contractors working for, and in many

cases in, the US intelligence community in cyber-espionage operations are even more difficult to place in an international legal framework.[41] The *Tallinn Manual 2.0*, extending the potential coverage of international law governing cyber operations to peacetime legal regimes, avoids identifying the elephant in the room, stating that peacetime cyber espionage is not per se regulated by international law.[42]

In Israel, the defence of the nation relies heavily on both society and business. Universal conscription underlines the citizen-soldier character of the Israel Defense Forces (IDF). Civil–military dependence also extends to the relationship between the military and industry. If anything, cyber security intensifies these civil–military ties as the country aims to be a central player in the international cyber-security industry.[43] The famous 'revolving door' that is symptomatic of relations between government and the defence industry in the US defines the cyber-security 'industrial complex' of Israel as well. According to the *Financial Times*, there are 'few other countries where the military establishment mingle so closely with academia and business, to all three sectors' profit', and the IDF's Unit 8200 – the SIGINT service that also conducts cyber operations – is at the centre of it all.[44] The intimate relationship between its veterans and the booming Israeli high-end security start-up community – combined with the strong tradition of reserve forces – provides a potentially powerful mixture of private contracting and a 'whole of nation' approach to cyber security and cyber operations.[45] As Maurer indicates, such a high level of integration raises questions about the long-term viability of norms that are built on the public–private distinction.[46]

In China, the People's Liberation Army (PLA) has always been emblematic of the citizen-soldier model, even though the organisation answers to the Communist Party rather than the state or the people.[47] Three developments characterise the Chinese model of operating in cyberspace. Firstly, the activity and importance of 'patriotic hackers' have declined relative to the operations of state agencies. Prolific in the early and mid-2000s, vigilante hacker groups have been reined in by the government, while the PLA has vastly expanded its operations. Secondly, a marked shift has occurred from what GCHQ director Iain Lobban described as 'industrial espionage on an industrial scale' to more targeted and subtle operations, and on a much

more limited political and economic scale.[48] The massive theft of Western intellectual property was temporarily stemmed by Mandiant's APT 1 report in 2013, the FBI's indictment of five PLA officers the following year, and the summit between US president Barack Obama and Chinese President Xi Jinping in 2015. For Xi, the public shame of the US indictment coincided with his own effort to reassert his control of the PLA by culling its business interests and ensuring its loyalty.[49] These reforms prepared the ground for the third development: a new realignment between the PLA units conducting cyber operations and the civilian Ministry of State Security responsible for foreign intelligence. China did not have a long tradition of investing in foreign espionage, having focused predominantly on internal security, but has professionalised its intelligence acquisition in the last two decades. The PLA's cyber operations have been consolidated and centralised in the Strategic Support Force to ensure better support for military operations, while the Ministry of State Security has been running more sophisticated APTs. As the role of the citizen-soldier hackers has diminished, the importance of the business sector, including high-tech companies such as Huawei and ZTE, has grown.[50] As with the US and Israel, the public sector in China seems unable to function without the private sector's cyber capacity.[51] The difference is that in China, the private sector remains subservient to the state.

Political and economic espionage has been outsourced

Russia has a long history of using proxies in cyberspace. The 2007 Distributed Denial of Service (DDOS) attacks on Estonian websites involved patriotic hackers coalescing with criminal elements to conduct operations that were at the very least condoned by the Russian state.[52] Many links between cyber crime and the state have since surfaced. Firstly, Russian criminal malware has been discovered that incorporates espionage functionalities (Gameover Zeus), or was adapted for sabotage purposes (BlackEnergy).[53] Secondly, there are several examples of criminal hackers being recruited as employees of the security services. Thirdly, as shown by the Yahoo hack in 2013–14 and the subsequent FBI indictment, political and economic espionage has been outsourced to criminal hackers.[54] This fits into

the broader picture whereby, according to Mark Galeotti, the Russian state has subsumed the underworld, ruling by decree when it can, and criminal violence when it must.[55] At the heart of the intersection between the state and the underworld lie the nation's security services, and it is no coincidence that those that hail from these units – the *siloviki* – hold the reins of power in contemporary Russia. Although patriotic hackers and criminal networks are harnessed to serve the interests of the state, the Russian Federal Security Service (FSB) is deeply involved in hacking operations, and entities it has enlisted have been heavily sanctioned by the United States. The main APTs appear to be run from the intelligence and security services. The civilian foreign-intelligence service (SVR) is known for its refined espionage operations (APT 29). The military-intelligence agency (GRU) runs the aggressive APT 28, its espionage operations frequently mutating into sabotage and subversion. The hack of the Democratic National Committee is a good example. APT 29 had been spying on the organisation months before APT 28 intruded and transferred the stolen data to WikiLeaks, manipulating the US electoral processes.[56]

The wrong track?

In view of state practices in cyberspace, leading non-governmental organisations, scholars and analysts may be on the wrong track in attempting to regulate behaviour. The key actors are foreign-intelligence agencies and private proxies. The United Nations Group of Governmental Experts did at least mention proxies in its 2013 report, stating that 'states must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs [information and communication technologies].'[57] Foreign-intelligence agencies and espionage activities, however, were barely mentioned, and certainly were not made subject to proposed norms. A legal and normative process that fails to address the primary actors in a given field is not a viable approach in the long run.

On the issue of proxies, two measures are crucial. Firstly, states must themselves review and specify the relationship between their military and intelligence agencies, on the one hand, and the cyber–industrial complex, on

the other. If distinctions between procurement and consulting, and between weapons and operations, are fading, new rules are required to delineate civil and military responsibilities. Secondly, the cost–benefit equation needs to be altered for states using illegal proxies to conduct malicious activities in cyberspace. Given that deniability, as opposed to the projection of power, is the main advantage gained from the use of these proxies, logic dictates that removing that advantage could alter the calculus of political utility. The trend in both Russia and China points to less reliance on criminal proxies and patriotic hackers, the countries' intelligence services being primarily responsible for quantitative and qualitative increases in cyber activities. For both illegal proxies and espionage activities that deviate from 'acceptable practice', naming and shaming through attribution can change the calculus for the attacker. The idea of imposing costs to deter malicious actors from blatant transgressions of acceptable state behaviour, such as attacking critical infrastructure or manipulating elections, is acquiring mainstream traction. By increasing the cost of cyber attacks, the calculus for the defender may change too. If a well-founded and credible case of public attribution risks the loss of an intelligence source, that loss might be a lesser evil than the continued impunity of the aggressor.

Finally, states need to address the issue of espionage. Intelligence agencies have not only been responsible for a host of cyber attacks, but in many countries have also become the hub of expertise in cyber defence. The UK and Canada, for example, are making their SIGINT agencies the one-stop shop for all national cyber-defence activities, and many countries have embedded government computer-emergency response teams in the intelligence community.[58] Cyberspace has thus facilitated the diversification of spying activities beyond traditional espionage, with responsibilities ranging from the protection of government networks to executing offensive cyber operations abroad. States have traditionally been reluctant to address espionage in international forums, privileging the freedom of manoeuvre that silence afforded. Over time, however, the widening gap between state practice and the putative legal framework is not tenable. States are increasingly regulating intelligence activities at the national level. Solving the conundrum of cyber conflict and intelligence would require them to restrict their

foreign-intelligence agencies purely to espionage. This is as unrealistic in cyberspace as it is in international relations. States, in general, are reluctant to unilaterally limit their own capabilities.[59]

An international framework therefore needs to be considered. For the past 100 years, an evolving body of international law and custom has shaped and restricted military activities. It is now time to start the process for espionage.

Notes

1 Isabelle Duyvesteyn, 'Between Doomsday and Dismissal: Collective Defence, Cyber War and the Parameters of War', *Atlantisch Perspectief*, 20 October 2014.

2 Compare Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010) with Thomas Rid, *Cyber War Will Not Take Place* (London: C. Hurst and Company, 2013).

3 See Myriam Dunn Cavelty, 'The Militarisation of Cyberspace: Why Less May Be Better', in C. Czossceck, R. Ottis and K. Ziolkowski (eds), *4th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2012); and Ronald J. Deibert, 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace', *Millennium: Journal of International Studies*, vol. 32, no. 3, 2003, pp. 501–30.

4 Joseph Nye, Jr, 'Deterrence and Dissuasion in Cyberspace', *International Security*, vol. 41, no. 3, 2017, p. 50.

5 See Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford: Oxford University Press, 2017).

6 See Lucas Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security*, vol. 38, no. 2, 2013, pp. 7–40; Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, vol. 35, no. 1, February 2012, p. 5; and John Stone, 'Cyber War Will Take Place!', *Journal of Strategic Studies*, vol. 36, no.1, February 2013.

7 Michael Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013); Michael Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

8 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN General Assembly, Doc. A/70/174, 22 July 2015.

9 See Alex Grigsby, 'The End of Cyber Norms', *Survival*, vol. 59, no. 6, December 2017–January 2018, pp. 109–22.

10 Rory Corman and Richard Aldrich, 'Grey Is the New Black: Covert

Action and Implausible Deniability', *International Affairs*, vol. 94, no. 3, May 2018, pp. 477–94.

11 Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security and the Copenhagen School', *International Studies Quarterly*, vol. 53, 2009, pp. 1,155–75.

12 Gary D. Brown and Andrew O. Metcalf, 'Easier Said than Done: Legal Reviews of Cyber Weapons', *Journal of National Security Law & Policy*, vol. 7, 2014, pp. 115–38.

13 See Corman and Aldrich, 'Grey Is the New Black: Covert Action and Implausible Deniability'.

14 See, for example, Ashley S. Deeks, 'Confronting and Adapting: Intelligence Agencies and International Law', *Virginia Law Review*, vol. 102, no. 3, 2016, pp. 599–685; Craig Forcese, 'Pragmatism and Principle: Intelligence Agencies and International Law', *Virginia Law Review*, vol. 102, no. 1, 2016, pp. 67–84; and Alexandra H. Perina, 'Black Holes and Open Secrets: The Impact of Covert Action on International Law', *Columbia Journal of Transnational Law*, vol. 53, no. 3, 2015, pp. 507–83.

15 Rid, 'Cyber War Will Not Take Place'.

16 See, for example, the cyber-operations tracker maintained by the Council on Foreign Relations, https://www.cfr.org/interactive/cyber-operations. The most convincing forensic evidence is often made public by private security firms. Most of these firms are Western, and focus on APTs from China and Russia. Some non-Western firms, such as Kaspersky, are considered untrustworthy. See Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies*, vol. 38, nos 1–2, 2014, pp. 4–37.

17 See James P. Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War', *Survival*, vol. 53, no. 1, February 2011, pp. 23–40.

18 David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012).

19 See Ryan Gallagher, 'Operation Socialist', *Intercept*, 13 December 2014, https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/.

20 Andy Greenberg, 'The Code that Crashed the World', *Wired*, September 2018, pp. 52–63.

21 Stilgherian, 'Blaming Russia for NotPetya Was Coordinated Diplomatic Action', *ZDNet*, 12 April 2018, https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/.

22 See, for example, Jack Goldsmith, 'The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance', *Lawfare*, 19 December 2014, https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance.

23 See David E. Sanger and Katie Benner, 'U.S. Accuses North Korea of Plot to Hurt Economy as Spy Is Charged in Sony Hack', *New York Times*, 6 September 2018, https://www.nytimes.com/2018/09/06/us/politics/north-korea-sony-hack-wannacry-indictment.html.

24 Ash Carter, 'A Lasting Defeat: The Campaign to Destroy ISIS', Harvard Belfer Center Special Report, October 2017, p. 33, https://www.belfercenter.org/sites/default/files/2017-10/

Lasting%20Defeat%20-%20final_0.pdf.

25 See, for example, Chris Bing, 'Command and Control: A Fight for the Future of Government Hacking', *Cyberscoop*, 11 April 2018, https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/.

26 Brown and Metcalf, 'Easier Said than Done'.

27 See Darien Pun, 'Rethinking Espionage in the Modern Era', *Chicago Journal of International Law*, vol. 18, no. 1, Summer 2017, pp. 361–2.

28 See Perina, 'Black Holes and Open Secrets'; and Forcese, 'Pragmatism and Principle'.

29 See Brown and Metcalf, 'Easier Said than Done', p. 128.

30 Max Smeets, 'A Matter of Time: On the Transitory Nature of Cyberweapons', *Journal of Strategic Studies*, vol. 41, nos 1–2, February 2017, pp. 6–32.

31 Brown and Metcalf, 'Easier Said than Done'.

32 See Janice E. Thompson, *Mercenaries, Pirates and Sovereigns* (Princeton, NJ: Princeton University Press, 1994).

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

34 *Ibid*., p. 20.

35 See Elke Krahmann, *States, Citizens and the Privatization of Security* (Cambridge: Cambridge University Press, 2010), pp. 21–50.

36 See Shane Harris, *@War: The Rise of the Military–Internet Complex* (Boston, MA: Houghton Mifflin Harcourt, 2014); and Lillian Ablon, Martin C. Libicki and Andrea Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica, CA: RAND Corporation, 2014).

37 See Maurer, *Cyber Mercenaries*, pp. 73–6.

38 *Ibid*., pp. 14–16.

39 Vijah M. Padmanabhan, 'Cyber Warriors and the Jus in Bello', *International Law Studies*, vol. 89, 2013, pp. 288–308. See also Sean Watts, 'Combatant Status and Computer Network Attack', *Virginia Journal of International Law*, vol. 50, no. 2, 2010, pp. 391–447.

40 Schmitt (ed.), *Tallinn Manual*, Rule 35.

41 See, for example, Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing* (New York: Simon & Schuster, 2008).

42 Schmitt (ed.), *Tallinn Manual 2.0*, Section 5, Rule 32. See also Asaf Lubin, 'Cyber Law and Espionage as Communicating Vessels', in T. Minárik, R. Jakschis and L. Lindström (eds), *10th International Conference on Cyber Conflict – CyCon X: Maximising Effects* (Tallinn: CCD COE Publications, 2018), pp. 203–25.

43 See Dmitry Adamsky, 'The Israeli Odyssey Toward its National Cyber Security Strategy', *Washington Quarterly*, vol. 40, no. 2, 2014, pp. 113–27.

44 John Reed, 'Unit 8200: Israel's Cyber Spy Agency', *Financial Times*, 10 July 2015, https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c.

45 Alexander Klimburg, 'The Whole of Nation in Cyberpower', *Georgetown Journal of International Affairs,* vol. 11, 2010, pp. 171–9.

46 Maurer, *Cyber Mercenaries*, p. 154.

47 Nigel Inkster, *China's Cyber Power*, *Adelphi* 456 (Abingdon: Routledge for the IISS, 2016), pp. 88–93.

48 Gordon Corera, *Intercept: The Secret History of Computers and Spies* (London: Weidenfeld & Nicholson, 2015), p. 235.

49 See Mara Hvistendahl, 'The Decline in Chinese Cyberattacks: The Story Behind the Numbers', *MIT Technology Review*, 25 October 2016.

50 See Ana Swanson and Cecilia Kang, 'White House Considers Barring Chinese Telecom Sales as Tensions Mount', *New York Times*, 3 May 2018.

51 See Inkster, *China's Cyber Power*, p. 104; Maurer, *Cyber Mercenaries*, p. 108.

52 See Sheera Frenkel, 'Inside The Hunt for Russia's Hackers', *BuzzFeed*, 21 April 2017, https://www.buzzfeed.com/sheerafrenkel/inside-the-hunt-for-russias-hackers.

53 See Michael Schwirtz and Joseph Goldstein, 'Russian Espionage Piggybacks on a Cybercriminal's Hacking', *New York Times*, 12 March 2017.

54 Indictment, *United States vs. Dokuchaev*, US District Court for the Northern District of California, filed 28 February 2017, https://www.justice.gov/opa/press-release/file/948201/download.

55 Mark Galeotti, *The Vory: Russia's Super Mafia* (New Haven, CT: Yale University Press, 2018), pp. 257–8.

56 See Eric Lipton, David E. Sanger and Scott Shane, 'The Perfect Weapon: How Russian Cyberpower Invaded the U.S.', *New York Times*, 13 December 2016.

57 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN General Assembly, Doc. A/68/98, 24 June 2013.

58 Sergei Boeke, 'National Cyber Crisis Management: Different European Approaches', *Governance*, vol. 31, no. 3, July 2018, pp. 449–64.

59 See Dennis Broeders, 'Aligning the International Protection of "The Public Core of the Internet" with State Sovereignty and National Security', *Journal of Cyber Policy*, vol. 2, no. 3, November 2017, pp. 366–76.