The Notion of Cyber Operations

Ducheine, P.A.L.; Pijpers, P.B.M.J.

DOI
10.4337/9781789904253.00024

Publication date
2021

Document Version
Submitted manuscript

Published in
Research Handbook on International Law and Cyberspace

Citation for published version (APA):
THE NOTION OF CYBER OPERATIONS

P.A.L. Duchêne

B.M.J. Pijpers

Amsterdam Law School Legal Studies Research Paper No. 2020-09
Amsterdam Center for International Law No. 2020-08
The Notion of Cyber Operations

By: Paul A.L. Ducheine and Peter B.M.J. Pijpers*

Table of contents
1. Introduction ........................................................................................................... 2
   1.1. Apples and Pears? No, Just (Different) Goals! .................................................. 2
   1.2. The Military in Cyber? ...................................................................................... 6
   1.3. Aim, Perspective and Structure ........................................................................ 7
2. Diversity in Strategic Objectives .......................................................................... 8
3. Common Operational Means and Methods .......................................................... 11
4. Applicable Cyber Paradigms for States ................................................................. 11
   4.1 Coordination, Governance and Diplomacy ....................................................... 13
   4.2. Protection ........................................................................................................ 14
   4.3. Law Enforcement ............................................................................................. 16
   4.4. Intelligence & Counter Intelligence ................................................................ 17
   4.5. Military Operations and Conflict .................................................................... 19
5. Response mechanism............................................................................................. 21
6. Operationalizing Cyber Operations ....................................................................... 22
7. Operationalizing Military Cyber Operations ...................................................... 23
8. Conclusion ............................................................................................................ 25

Abstract
The aim of this chapter, is to elaborate on the notion of ‘cyber operations’ as they seem to be used in a generic manner in popular media as well as in academics. This chapter differentiates for actors and motives, covering operations conducted by both state and non-state entities. Special attention will be paid to governmental cyber operations that are characterized by five distinct roles and paradigms: governance, protection, law enforcement, intelligence and military operations. In addition, governmental response mechanisms, based on the paradigms, are explained and operations themselves are operationalised.
Despite similarities regarding means and methods used in all these cyber operations, the fundamental distinction lies in the purpose of those launching these activities. For governmental actors, the purposes are vested in the aforementioned paradigms.

* Brigadier-General Paul A.L. Ducheine, PhD, LL.M., MSc (Army Legal Service) is a Professor of Cyber Operations at the Netherlands Defence Academy (Faculty of Military Sciences), Professor of Law of Military Cyber Operations at the University of Amsterdam, and researcher at the Amsterdam Centre of International Law. Colonel Peter B.M.J. Pijpers, LL.M, MSc (Army Logistic Corps) is an Associate Professor of Cyber Operations at the Netherlands Defence Academy and PhD researcher at the Amsterdam Centre of International Law. The authors are grateful for the comments delivered by Prof. Terry Gill, Mark Roorda, Willem van Poll and Dr. Jelle van Haaster.
1. Introduction

1.1. Apples and Pears? No, Just (Different) Goals!

The concept of cyberspace, some 35 years ago coined by William Gibson, can be understood as “to cover all entities that are or may potentially be connected digitally”. Ever since the activities executed within this cyber domain have often been framed in belligerent terms associated with conflict and attack, implying a malign nature full of warlike threats. But let’s put this in context both for State and non-State entities.

Cyberspace is not merely used for malign purposes. In fact, most activities have a benign character related to commercial and private uses of the internet and social media. Moreover, various assessments reveal that not ‘cyber war’, but digital espionage and cybercrime have been, and remain to be the biggest threats to both government and the business community.

The 2013 Snowdon files have shed light on the covert activities of governmental intelligence agencies around the world conducting operations in and through cyberspace. This appears self-evident for public (or governmental) agencies, however, the number of private enterprises digitally collecting and providing information is growing steadily. Activities of intelligence agencies and private companies include social-media monitoring, digital investigation, and ordinary marketing research. Most notably, large ICT-companies such as Google, Microsoft and applications like Facebook, WhatsApp, Twitter, Instagram,

---


2. See Netherlands Defence Cyber Strategy (2012), UK version: “Cyberspace is understood to cover all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases relates in some way to the data (source code, information, etc.) present in this domain”. Original: Parliamentary Papers II 2011-2012, 33 321, no. 1.


5. For the description of cyberspace used in this chapter, using a model with three dimensions (cognitive, virtual and physical) and sub-divided in seven layers consisting i.a. social groups, psyche, cyber-identities, cyber-objects, hardware, objects and geographical locations (of all entities). See Paul AL. Ducheine and Jelle van Haaster, ‘Fighting Power, Targeting and Cyber Operations’ (2014) 2014 International Conference on Cyber Conflict, CYCON 303.; Paul AL. Ducheine, Jelle van Haaster and Richard van Haruskamp, ‘Manoeuvring and Generating Effects in the Information Environment’ 155.

6. For instance, services provided by Information Security firms, see Mandiant’s Intelligence Centre <www.mandiant.com/products/intelligence-center>, well known for reporting on China’s alleged Advanced Persistent Threat, the Dutch niche company Fox-IT <www.fox-it.com/en>.


Zoom and LinkedIn are also collecting data for (future) business purposes. Google’s knowledge of search-queries enables it to know more details about individuals than these people know (or realize) themselves. This data can be utilised to micro target customers into persuading them to purchase products (i.e. marketing), for investigative journalism (i.a. Bellingcat), to monitor Corona-virus lockdown rules, but the same techniques are also used to sway voter preferences. Since a number of these ICT companies are being observed by, collaborate with or are forced to work with governmental intelligence agencies, this private (and economic) information is likely also available for the latter.

Next to espionage and intelligence, the other substantial threat originates from a group of actors that bear no public responsibility at all: criminals who use cyberspace as a vector for their actions, as a target for their activity, as a line of communication, or as a marketplace to sell their ‘products’ on the so-called dark web. In order to counter this threat, stakeholders varying from individuals to Internet Service Providers, from anti-virus vendors to governments, have taken a variety of countermeasures. These measures may be preventive in nature by installing firewalls and anti-virus software, by penalising cybercrime by implementing the Budapest Cybercrime Convention, or through participation in the

---

9 Recently, a number of those companies advocated more restrictions on governmental surveillance and reform of legislation in this respect. See <www.reformgovernmentsurveillance.com>.


UNODC supported workgroup on preventing and combatting cybercrime.\textsuperscript{16} In addition, governments are preparing responses by drafting legislation enabling law enforcement officials to ‘hack-back’, once designated forms of (cyber) crime have been discovered.\textsuperscript{17}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{cyber_threat_landscape.png}
\caption{Cyber threat landscape}
\end{figure}

However, apart from espionage and crime, cyberspace is also used for a variety of other purposes. According to David Sanger, the US and Israel produced and used the famous Stuxnet virus against nuclear production facilities in Iran, delaying its nuclear program and thereby biding time and preventing (or postponing) a physical (military) aka ‘kinetic’ operation against Iran’s nuclear program.\textsuperscript{18} This form of cyber sabotage or ‘cybotage’,\textsuperscript{19} was a complicated, multidimensional and costly operation against an Industrial Control System (ICS) not connected to Internet and therefore physically protected by (inter alia) a so called ‘air gap’. This, however, didn’t hamper the operation and might become even more likely since researchers have now evidenced that acoustic signals may also cross


\textsuperscript{19} John Arquilla, ‘Cyberwar Is Already Upon Us - But can it be controlled?’ (\textit{Foreign Policy}, 2012) <http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us#sthash.OffAFk4W.dpbt> accessed 1 March 2014.
air gaps like these. Hence, cyber activities have had effects in the physical domain, and will have, with reference to the 2015 and 2016 sabotage of the Ukrainian power grid. Finally, cyberspace also features and supports warfare, war-related activities and (other) military operations. Already in 2007, Syrian air defences didn’t notice Israeli jets bombing a nuclear facility at al Kibar. Apparently, the air defences were manipulated from outside, using cyberspace as an entrance and digital code as tooling. During the Second Gaza War (2012), Israel Defence Force (IDF) and Hamas were battling in cyberspace, using blogs and tweets as instruments in an information campaign. Sympathisers (or victims) expressed their feelings and ideas as well. Characteristic for cyberspace, geographical dislocation doesn’t hamper groups and individuals from joining conflicts (and other forms of social behaviour), thus confronting or supporting the warring parties digitally. Hackers bearing the name Anonymous, launched their ‘#OpIsrael’, defacing and obstructing Israeli websites and e-services, or declaring ‘war’ against ISIS and taking control of hundreds of ISIS Twitter accounts. Thus, Anonymous and (h)activist groups alike have entered the realm of conflict, partially in pursuance of their ‘corporate’ mission, but by launching virtual (i.e. cyber) operations, also entering the domain of operations that are closely related to the physical military conflict that is being fought by the warring factions as well.

Cyber operations as displayed above are executed by both State and non-State entities. Though the objectives may differ, the activities are similar, varying from digital

20 Michael Hanspach and Michael Goetz, ‘On Covert Acoustical Mesh Networks in Air’ 8 Journal of Communications 758.
22 Peter Warren Singer and Allan Friedman, Cybersecurity and Cyberwar - What everyone needs to know (Pb edn, Oxford University Press 2014) 126-128.
24 For instance, <occupiedpalestine.wordpress.com/2012/11/18/gazaunderattack-nov-18-2012-liveblog/>.
28 I.e. in the factual meaning, without necessarily (directly) participation in the hostilities.
espionage; criminal and subversive acts including DDoS-attack, hacking and leaking operations, defacements and destruction of data; up to acts that have an effect in the physical world, be that in war or situations short of war.

Whichever source is behind these threats, irrespective of the motivation that is driving such cyber activities, and regardless where and against what or whom they are conducted or directed, the common denominator of these forms of social behaviour, seems – at first glance – to be a military and warlike one, as all of them are referred to as ‘attacks’, the activities quite often labelled as ‘operations’, and the total once and again is characterized as ‘cyber warfare’, making comparisons with the Cold War\(^29\) or refer to an arms race in cyberspace,\(^30\) as if the whole phenomenon were militarized.

1.2. The Military in Cyber?

However, despite the belligerent language often used,\(^31\) in reality, the portion of military involvement in cyber activities seems fairly limited. This, yet, ought to be nuanced. This observation may be true regarding cyber warfare proper, i.e. the conduct of military cyber operations in the context of an armed conflict in the legal meaning.\(^32\) Yet, as cyber operations may not – and most times do not – qualify as cyber warfare proper, other cyber operations are characterized by military involvement as well. Therefore, the military’s contribution to cyber operations is larger: quantitatively and qualitatively.

First of all, the military portion may be larger in numbers (quantity), as some states have provisions whereby the military are involved through non-military institutional arrangements. Some of the military intelligence and security services operate under civil (i.e. non-military) legislation and control. Some of the intelligence services have a dual role: civil and military tasking alike. In addition, some states have a role for military police forces within the law enforcement domain.

Secondly, although small in numbers, the military may play a crucial and inevitable role in the providing ‘cyber security’. Nowadays, governments increasingly rely on a multidisciplinary or inter agency approaches to (modern) security threats as is clearly visible in counter-terrorism and cyber-security policies, thus using the ‘whole of government’ to face and address modern threats.

Moreover, some States decided that an active and forward presence in their digital defence with other (State and non-State) actors beyond the territorial boundaries of their own cyber-infrastructure cannot be executed without military assistance.\(^33\) The purpose of this so-called ‘persistent engagement’ in cyberspace is the surveillance and monitoring of

---


(potential) threats based on tacit agreed competition of cyber activities below the threshold of the use of force.\textsuperscript{34}

1.3. Aim, Perspective and Structure

Suitable or not, the term cyber operation seems to become a common denominator for activities in cyberspace, undertaken with the aim of achieving objectives in or through this digital domain. The common denominator can be used in a great variety of situations, by a diversity of actors and, quite obvious, for various reasons.

The aim of this contribution therefore, is to elaborate on this notion of ‘cyber operations’ as they seem to be used as a universal, a rather generic and non-specific term. As a starting point, the definition offered by the Tallinn Manual international group of experts will be used for this purpose. Cyber operations are defined as: “The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace”.\textsuperscript{35}

The primary perspective will be that of the State, the principal subjects of international law.\textsuperscript{36} However, as demonstrated above, since non-State entities are on par in this domain or even exceed States in activities, attention will also be paid to the characteristics of cyber operations conducted by non-State actors.

Although not all non-State actors may have explicitly formulated a formal strategy as States (normally) do, some will have an implied, rudimentary articulated ‘corporate goal or end’.\textsuperscript{37} Whether communicated explicitly or not, and regardless of its legitimacy, State and non-State actors alike allocate resources (means) and undertake activities (ways) in order to achieve those designated goals or ends.\textsuperscript{38} In doing so, non-State actors (at least rational ones) and States both use strategic objectives at the ‘corporate’ or ‘strategic’ level of their organisation. These strategic objectives are subsequently implemented by subordinate entities at the operational (or tactical) level through the allocation of means, and the definition of ways to employ the latter. These two characteristics of organisations – objectives and means & methods – will be used to describe differences and similarities in the various cyber operations.


First, for state and non-state entities alike, the differences in objectives at the strategic level will be displayed (Section 2). Section 3 will then reveal similarities at the operational level, being the ‘means and methods’ used to achieve these strategic objectives. Subsequently, the primary focus will be on state actors, displaying the distinct roles of states by articulating five strategic paradigms used to characterize cyber activities, their purposes and institutional frameworks (Section 4). Section 5 then operationalizes cyber operations (in general) and military cyber operations in particular (Section 6) by describing its specific features and phases.

2. Diversity in Strategic Objectives

States and non-state entities (at any rate lucid ones) alike will be inspired or driven by implied or publicly stated institutional (i.e. national or corporate) strategy. Even when ostensibly merely reacting on ‘events’, state and non-state activities will be driven or guided by (some basic form of) strategic imperative. This is also true for activities in cyberspace. These strategic imperatives may be ‘plain and simple’, for instance economic profit, or complex, ranging from enhancing cyber security – as (inter alia) crucial and critical public and private infrastructure or services are reliant on ICT – to achieving military superiority in cyberspace.

The primary aim of states will be to enhance (national) security and to promote and safeguard their (other) vital national interests. These vital interests may be stated in a grand or national security strategy, or they may be implied in or deducted from national (security) policies,39 some explicitly focussing on cyber security issues.40 As cyberspace is interconnected with other domains, and vital interests are increasingly interrelated and dependant on ICT and digital networks e.g. the internet, security in cyberspace (hence cyber security) is a vital strategic interests in its own right (see Figure 2), as also alluded in the

---


Netherlands National Security Strategy. Examples of the inextricable connection between the vital interests in the digital domain is the hack into the Netherlands’ Diginotar case.

Figure 2: National security and its vital interests (for the Netherlands)

Looking at non-state actors, their strategic notion may differ from that of states and often originates from commercial or ideological incentives. Regarding legitimate commercial enterprises, their goal will be economic profit, as it is the case for Kaspersky, Norton, Symantec, Google, Facebook et al. Of particular interest are commercial enterprises that appear to be supplying tools enabling others to conduct cyber activities. Cyber activities

---

41 Netherlands National Coordinator Terrorism & Security, ‘National Security Strategy’ (2019). 12 stating that “As national security can also be affected via cyberspace, cybersecurity has been interwoven into all of the other national security interests.”


43 E.g. “Symantec’s mission is to make the world a safer place by protecting and managing information so everyone is free to focus on achieving their goals. It’s a statement that ties our business goals to a social purpose as we help people, businesses, and governments secure and manage their information-driven world against more risks at more points, more completely and efficiently than any other company.”, at: <www.symantec.com/corporate_responsibility/topic.jsp?id=ceo_letter>, accessed: 29 December 2013.

are part of their business model, if not their product.\textsuperscript{45} Actors with a specific malign intent, such as hackers executing an Advanced Persistent Threats (APT) which can be cyber criminals seeking intellectual property or financial information, to state-controlled or proxy ‘hackers for hire’ stealing data or compromising cyberinfrastructure. Non-profit organisations such as Bellingcat, the TOR-project, Anonymous or CCC,\textsuperscript{46} as well as thematic pressure groups such as Bits of Freedom, Privacy First or the Electronic Frontier Foundation will pursue political and/or ideological goals.\textsuperscript{47} Their cyber activities will be more focussed upon freedom of expression, transparency, free internet, net neutrality, privacy et cetera. Cyberspace may be at the heart of their strategic values, or may offer leverage as a vector or medium for their activities.

Ideology also seems to be the primary objective of non-state actors that have entered battlefields and conflicts digitally: Hamas, Hezbollah, the Syrian Electronic Army, and again, Anonymous \textit{cum suis}. Apart from ideology, some of these actors may also have other ambitions that may even resemble those of states: territorial or military. Recent events have demonstrated that non-state actors, with or without the sponsoring of affiliated states, have conducted numerous ‘cyber operations’ ranging from purely ideological (Estonia 2007; UK 2016, France 2017), in support of (or at least supportive to) military conflict (Georgia, 2008; Ukraine, 2014, 2015, 2016), autonomous (Anonymous, 2012) or as part of military conflict (Hezbollah, 2006; Hamas, 2012).\textsuperscript{48} In more than one respect, their operations are quite similar to cyber operations conducted by states (through their organs), and as such, these operations are as instrumental to corporate strategic aims, as they are for states.

In sum, state and non-state cyber activities, regardless of their legitimacy and legality under national and international law, potentially pose threats to what is defined as cybersecurity.\textsuperscript{49} When combined, these threats represent a threat landscape as depicted in Figure 1 above.

\textsuperscript{45} E.g. “It is Fox-IT’s mission to make technical and innovative solutions that ensure a more secure society. We do that through the development of advanced cybersecurity and cyberdefense services and solutions for our clients around the world. We achieve this through a strong focus on innovation and a tireless dedication to our clients, our values, and our integrity”, at: <www.fox-it.com/en/about-us/>, accessed 29 December 2013; also “Hold Security provides the best innovative services to meet your company’s needs.”, at: <www.holdsecurity.com>.

\textsuperscript{46} On Anonymous, see e.g. Coleman. See the German Chaos Computer Club or CCC, at <http://www.ccc.de/en/> accessed 18 March 2014.

\textsuperscript{47} E.g. “Privacy First takes a professional and evidence-based approach to the various issues. The preservation of liberty in the private sphere can be perfectly combined with rapidly changing societal and technological developments.”, at: <www.privacyfirst.eu/>, accessed 29-12-2013. “From the Internet to the iPod, technologies are transforming our society and empowering us as speakers, citizens, creators, and consumers. When our freedoms in the networked world come under attack, the Electronic Frontier Foundation (EFF) is the first line of defense”, at: <https://www.eff.org/about>.

\textsuperscript{48} For an update on cyber operations, see: https://www.cfr.org/interactive/cyber-operations

\textsuperscript{49} Cybersecurity is “the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes”. See: Cisco Systems. What is Cybersecurity? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
3. Common Operational Means and Methods

Although the strategic objectives of the various actors conducting cyber operations may differ, in general they use the same capabilities in terms of means and methods. This is demonstrated by the shared dependency on knowledge and skills that is required to conduct these activities. Thus, whether operating in governmental service (military and civil), commercial companies, pressure or activist groups, or in sheer isolation, all cyber operators or ‘hackers’—white, grey and black hats alike—require the same skills and expertise.

Apart from personnel, knowledge and skills as a prerequisite for cyber capabilities, the ways and capacities, or in other words, the means and methods to achieve strategic aims are comparable. All cyber operators will require similar (if not the same) tooling, software and hardware, whether it is their intent to provide legitimate services, to prevent misuse of cyberspace, or because misuse is their very goal. One of the clearest demonstrations of commonalities at the operational level vis-à-vis cyber means and methods is monitoring software (and hardware) that is used by CERTs, intelligence agencies, law enforcement official, military units, civilian cyber security companies, as well as organized criminal groups or hacktivist groups.

However, they may take opposing sides. Taking into account that the aims of cybersecurity companies (e.g. Symantec) and vendors (e.g. Microsoft) on the one hand, and cyber criminals on the other hand will be opposite, their ‘business-models’ or in other words, the operational ways to achieve goals, centre on the same lines of software and code. Where it is Symantec’s and Microsoft’s task to discover and/or to fix vulnerabilities, it is the criminal’s intent to exploit these very weaknesses.

Thus, despite strategic differences between states and (some) non-state actors, at the operational (and tactical) level, there appears to be more similarity as all actors—conceptually—rely on more or less the same basic requirements (personnel, knowledge and skills) and means and methods, that is: capabilities and capacities (see Section 5).

With this conclusion in mind, the next sections will take a state perspective as a starting point in order to further differentiate between the varieties of cyber operations.

4. Applicable Cyber Paradigms for States

Looking at cyber activities at the state level, a number of distinct paradigms are applicable to describe cyber operations: coordination & governance, protection, law enforcement, intelligence and military operations. These paradigms are demonstrated in national cyber security strategies worldwide, as well as through the instrumental use of cyber capabilities in furtherance of states’ (other) vital interests. These paradigms—related to the inherent governmental function to provide security and to further vital interests of the state—can be depicted as parts of a continuum,

50 AIV and CAVV at 15, 17, and 36.
51 When and where required, special attention will be paid to non-state actors conducting cyber operations, criminal activities excluded, although the analysis offered may fit their activities as well.
53 For an overview: see supra note 40.
54 E.g. Stuxnet, see: Sanger, supra note 18.
a spectrum, or to put it differently, as part of a state’s comprehensive efforts in cyberspace. The paradigms are complementary and overlapping.

These paradigms represent one (or more) of the institutional frameworks enabling governments (or public authorities) to conduct activities within democratic societies. They thus offer a legal and social framework for (governmental) behaviour that is, as with all social interaction, subject to adjustments that are initiated or inspired by changes in the security landscape (including ‘new’ threats), public opinion, international, societal and technological trends. As such, these frameworks reflect the Zeitgeist regarding topics that have reached the political agenda and require or enable governmental action.

In democratic states, adhering to the principle of the rule of law, these arrangements and organizations, at least when exercising public authority (that may interfere with civil liberties), will have a designated legal basis establishing the organisations and arrangements in the very first place. In addition, these arrangements and organization will have to execute their tasks and powers in accordance with legal regimes that are applicable once these activities are conducted. The designated legal bases and legal regimes, together with oversight mechanisms, authority and accountability rules, are part of the legal framework that characterizes the various paradigms.

The frameworks can be understood as the product of existing (inter)national law, political systems, political attention, public opinion, public demands, as well as (lack of) audacity and leadership. The frameworks are tangible through (institutional and ad hoc) arrangements and governmental organisations tasked with designated roles in cyberspace and cyber security.

The rise of these frameworks and paradigms, is evident when analysing states’ cyber security policies or strategies. Five core paradigms can be detected: coordination and (internet) governance including diplomacy, protection, law enforcement, (counter) intelligence, and military operations which include conflict. They will be explored subsequently below.

---

55 AIV and CAVV, at 16
56 Klimberg and Mirtl 15, referring to these paradigms as ‘mandates’.
59 Including counter-security.
Each of these paradigms provides a framework that represents public support, legal bases, legal regimes, and institutional arrangements. More than often, these frameworks are used in a complementary manner. Taken together they enable cyber operations throughout a wide and fluid spectrum, ranging from “the monitoring of governmental networks by Computer Emergency Response Teams or CERTs, to active protection by shutting down sites once they are under ‘attack,’” and followed by “criminal investigations into the source of the ‘attacks’ where criminal activity was reasonably suspected”. These operations may be combined with “intelligence operations to inter alia ascertain the nature of the threat posed and identify the source of the threat, possibly resulting in a military response in situations which rose to the level of a use of armed force by a foreign power or organized armed group, even resulting, in exceptional cases, in participation in an armed conflict”.

4.1 Coordination, Governance and Diplomacy

Although this framework doesn’t comprise actual cyber activities, coordination first of all refers to internet governance, diplomacy and to national and international efforts to shape (governance in) the digital domain. As cyberspace – unlike physical domains – is

---

61 As, for instance, in counter-terrorism, see: Paul A.L. Ducheine and others, (n 60) 110.
62 Paul A.L. Ducheine and others, (n 60) 110.
characterized by a dominant role for non-state actors, both private and non-
governmental, the role of states is thus different compared to the physical world, and to
a certain extent rather limited, although not irrelevant. The added value of states in this
domain lies, *inter alia*, in the use of ‘classic’ instruments such as bilateral of multilateral
treaties, cooperation, as well as in their position in governmental and non-governmental
bodies such as the EU, UN or ITU. Secondly, coordination refers to national
coordination between the public and private organisations contributing to the other four
paradigms. Agencies such as the French ANSSI, the UK’s GCHQ or the Netherlands’
NCSC have a coordinating role directing governmental departments, and advising and
guiding private actors. It is fair to say, that state activities in the field of internet governance
are pro-active and preventive in nature, and are part of states’ overall cyber security
interests and strategies.

4.2. Protection

The second paradigm for state activities in the cyber domain is related to the protection of
(critical) cyber infrastructure. In part this refers to ‘ordinary’ critical infrastructure such as

---

67 Eric Luijif and Jason Healey, ‘Organisational Structures and Considerations’ in Alexander Klimburg
Cyberspace’ in Katharina Ziolkowski (ed), *PeaceTime Regime for State Activities in Cyberspace International
Law, International Relations and Diplomacy* (NATO CCD COE 2013).
69 E.g. Convention on Cybercrime.
70 E.g. NATO’s efforts through its cyber defence policy, NATO, ‘Chicago Summit Declaration, Issued
by the Heads of State and Government participating in the meeting of the North Atlantic Council in
declarations and outcome documents: Geneva 2003 (Geneva Declaration of Principles and Geneva
Plan of Action) and Tunis 2005 (see supra note 63).
to develop a hub for expertise on international law and cyber security”. See e.g. the involvement in the
UNGGE and OEWG, United Nations General Assembly, Resolution on establishment of OEWG -
A/RES/73/72 of 5 December 2018; United Nations General Assembly, Resolution of establishment
76 Protection is thus one perspective in order to promote the wider notion of overarching ‘security’. 

14
electricity or waterworks as far as this infrastructure is connected with or processed through cyberspace. Originally, critical infrastructure protection (CIP) refers to, primarily, physical protection against accidents, disasters, technical or human failure, and crime.

In addition, vulnerabilities in the digital domain itself, referring to the logical layer, may be the focal point of (in)security issues, regardless whether these breaches had a technical or human trigger, or whether they are the result of accidental or deliberate events. Serious cyber incidents may lead to major disturbances and disruption of society.

But the protection of infrastructure also entails deliberate violations due to remote cyber-attacks resulting in damage or the loss of functionality of the infrastructure. Cyber incidents in Estonia (2007), the spread of the Stuxnet virus (2010) but also the (Not)Petya (2016/2017) and WannaCry (2017) attacks have had a direct or indirect effect on CIP as well. Since many of the critical or vital services and installations are controlled through or depending on cyberspace, security in the digital domain is becoming ever more important.

Protection as a paradigm refers to a range of state activities, varying from resilience, redundancy, to prevention (legislation, imposing incentives for ‘hardening’, physical protection, firewalls, DMZs, and technical standards) all the way to countering security breaches. The establishment of Information Sharing and Analysis Centres (ISACs) and CERTs is just one of the examples. Looking at the nature of the critical infrastructure and that of cyberspace in particular, it is evident that public-private cooperation is a prerequisite for states in order to ensure effective (implementation of) cyber security policy.

Of particular interest is the issue of ‘governance’ in protective perspective. Various ideas, i.a. ‘notice and take down’, have been proposed and criticised, demonstrating the delicate equilibrium in the public-private domain as these ideas require support from essential private partners. However, over time, responsible disclosure policies, and even mandatory reporting of breaches (in vital sectors) and through privacy related mechanisms have been enacted. Although some legal and legislative issues are covered by other paradigms (e.g. law enforcement and military operations) it is fair to say that the role of protective powers and countermeasures is not as sophisticated in cyberspace as they are in other domains. To date, more than once, states have enacted legislation empowering private security companies in the physical world to provide armed services. Security is thus – once more – no longer the exclusive domain of state actors. As mentioned above, some commercial enterprises are rather active in cyberspace as well. Internet service providers (ISPs) and other digital services alike, play a pivotal role in this paradigm as well. Where consumers and organisations (small and large) fail to secure their ICT systems in an

79 The Stuxnet-virus was designed to infect a so-called Industrial Control System (ICS) that was not connected with internet.
80 See e.g. the policy of the British Library (a non-departmental public body): <http://www.bl.uk/aboutus/terms/notice/> accessed 18 March 2014.
82 E.g. in the field of counter-piracy: see Bibi van Ginkel, Frans-Paul van der Putten and Willem Molenaar, State or Private Protection against Maritime Piracy? A Dutch Perspective (Clingendael Centre for International Relations 2013).
effective manner, these services are at the front of fighting spam, malware or unauthorised intrusions.\textsuperscript{83}

Though protection is defensive in nature, a more active posture is chosen by some States, based on the postulation that cyberspace is inherently hostile. According to this stance, it is required to increase resilience, defend beyond the limits of national infrastructure and persistently engage with state and non-state entities acting in a similar way.\textsuperscript{84} Despite its terminology, this stance doesn’t seem to fit well in the ‘protection paradigm’. From its content, the stance probably uses a combination of the law enforcement, intelligence and even military operations paradigm too.

However, apart from the other arrangements related to the law-enforcement, intelligence or military operations paradigm, state and private contractors usually lack powers to actually execute cyber operation from a protective perspective. Interestingly though, these powers frequently have been made available in the realm of physical security, for instance in the field of guarding military infrastructure.\textsuperscript{85} Paradoxically, Dutch military guards may thwart an attack against physical military infrastructure, even with the use of lethal force,\textsuperscript{86} whereas the Dutch Defence CERT is not empowered to use digital force to repel or stop cyber-attacks against MoDs digital infrastructure and data, including networks. Until now, such defensive measures, or to put it alternatively, cyber operations, would be the exclusive realm of other paradigms such as law enforcement or intelligence.

4.3. Law Enforcement

Law enforcement is (thus) one of those alternative paradigms for states, providing for preventive measures by penalizing cybercrime, repressive measures by empowering law enforcement agencies to conduct investigations and so forth. The law enforcement paradigm “comprises a wide set of organisations” at various levels, i.e. national and international,\textsuperscript{87} local and national, and various governmental agencies and departments,\textsuperscript{88} i.a. national police, EUROPOL, ministries of justice, internal affairs but also defence for military police; railway and traffic police. To be effective, public-private partnership may be required, as well as cooperation with national (and other) CERTs and public-private ISACs, as well as intelligence and security services.

Apart from (harmonizing and) penalizing cybercrime, enforcement powers in the digital domain require amendments as well. To date, even ‘classic’ crime investigations heavily relies on digital investigative techniques, as physical pieces of evidence are increasingly superseded by digital ones.\textsuperscript{89} When cybercrime is involved, additional enforcement and investigative powers will be essential to enhance effective policing and


\textsuperscript{84} United States Cyber Command (n 34), 6.

\textsuperscript{85} See Duchêne and others (n 60) 114-115. For a European overview of such powers: Georg Nolte (ed) European Military Law Systems (de Gruyter Verlag 2003).

\textsuperscript{86} Article 1 of the Act on the Use of Force by Guards of Military Objects (in: Staatsblad 2003, 134).

\textsuperscript{87} Tiirmaa-Klaar (n 64), 520.

\textsuperscript{88} Luijif and Healey (n 67), 122, referring to ‘mandates’ instead of paradigms.

prosecuting. Thus, states have enacted additional legislation, e.g. the Netherlands, the UK and others.

As in any other domain, powers to execute cyber activities for law enforcement purposes, will require public support, at least political support, resulting in legislation providing a legal basis and applicable legal rules or a code of conduct (i.e. legal regimes). The legal framework is a common requirement derived not only from the principles of democratic states, but more in particular from obligations resulting from international human rights treaties or customary law.

Apart from the delicate issues of balancing intrusive powers with human rights, especially privacy and freedom of expression, the other main dispute concerns the extra-territorial application of these law enforcement powers, e.g. when hacking back is used as a method by the police. Public international law principles such as non-intervention and the sovereign rights of states will be major points of reference in this respect.

4.4. Intelligence & Counter Intelligence

Apart from, and in addition to the law enforcement paradigm, states also rely on a classic security paradigm called intelligence (and counter intelligence), including espionage and countering security threats through intelligence and security organisations. Depending on institutional and constitutional arrangements, states have essentially similar tasking for their

---


91 For the Netherlands: a preliminary draft of the proposal on Cyber Crime III was published in the beginning of 2013, see: Blommestein. The draft-proposal is due to be presented to Parliament in the beginning of 2014. The draft (in Dutch) can be found at: <https://www.internetconsultatie.nl/computercriminaliteit/document/726> accessed 15 March 2014.


93 The Explanatory Note (Dutch: ‘Memorie van Toelichting’) to the Dutch preliminary draft proposal, refers to the situation in Belgium (Dutch: Wet inzake informatiecriminaliteit, Wet van 28 november 2000, Belgisch Staatsblad, 3 februari 2001, nr. 2909), France and Germany.

94 E.g. the Dutch preliminary draft proposal refers – rather briefly – to this controversial issue by stating “much will depend on the nature of the actual cyber enforcement activity [i.e. hacking back] whether or not public international law will legitimize the conduct of the law enforcement agencies” [Translation PD].

intelligence and security services. Their primary function is to gather and analyse information about threats directed against the state and its population. This is based on, and in accordance with applicable law and political guidance. Collecting information in and through cyberspace is complementary to the existing set of capabilities being used by these services.

After the terrorist assaults of 2001 (9/11), 2004 (Madrid) and 2005 (London), legislation has been amended (or at least drafted and proposed) to (more) effectively counter terrorist threats. This legislation also includes powers (and regulations) to gather information (or intelligence) through cyberspace, hence cyber operations. Amendments and supplements to the legal bases for these powers and activities, have been the result of a successful attempt to use the window of opportunity after 9/11. However, as a result of the joint revelations of whistle-blowers, journalists and activists, these powers and applicable regimes are up for public debate and legal review. This public and political attention will remain of influence to (future) cyber operations and renew, inter alia, the debate regarding necessity, effectiveness, human rights and so on.

Although most tasks for intelligence services are defensive in nature, a pro-active stance is also possible. Some states permit their intelligence services “to exploit the information for other purposes, or directly intervene in order to prevent threats from (re)occurring”. The earlier mentioned Stuxnet virus is probably one of the best-known cases in this respect. Actions undertaken by intelligence services to counter cyber threats – i.e. counter-intelligence – are a furtherance of those that can be found within the protective paradigm, or could be the start of a cyber operation that fits within the military (covert) paradigm.

---


97 Klimburg (n 74) 124.


Apart from national legislation, intelligence gathering is the subject of international legal attention as well. Although no prohibition of cyber activities per se of cyber espionage exists in international law, it is clear the intelligence activities in or through cyberspace (cyber operations) may affect various national jurisdictions in a number of ways. In addition to the fact that the operations may qualify as criminal offences according to domestic criminal codes, they may also involve violations of civil law, international private law (intellectual property rights) and trade law. Moreover, public international law may be implicated in a number of ways. First of all, diplomatic law is of influence. But more importantly, some of the general principles of international law, i.e. state sovereignty, non-intervention as well as the prohibition on the use of force have an effect on the legal framework within this paradigm. Compared to classic intelligence activities, the extraterritorial dimension, and thus the international law ramifications are more pronounced as cyber infrastructure is situated in various jurisdictions and states.

4.5. Military Operations and Conflict

The last – and in some respects the most extreme – of the five core paradigms for states is the one that could be characterised as military operations, including conflict. The paradigm comprises (a) warfare proper (the conduct of military operations within the framework of armed conflict) and (b) ‘operations other than war’ including peace support (and enforcement) operations related to conflict, but outside the framework of armed conflict.

Military cyber operations, quite often referred to as ‘cyber warfare’ in its generic meaning, have been preliminary defined (see: Section 1) as the “employment of cyber capabilities with the primary purpose of achieving [military, PD] objectives in or by the use of cyberspace”. These military objectives are translations of a state’s strategic objectives. Apart from the present author’s specification, this definition is rather broad.

Others definitions are more specific, e.g. the Dutch Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law, in their joint advice to the Netherlands Government, meaning: “the conduct of military operations to disrupt, mislead, modify or destroy an opponent’s computer systems or...”


105 For reasons of clarity and for the purpose of this contribution, the author refrained from using ‘warfare’ in its more generic meaning: the art of conducting military operations (including i.a. warfare proper).

106 For an illustrative summary of these operations, see Terry D. Gill and Dieter Fleck, The Handbook of the International Law of Military Operations (Oxford University Press 2010).

107 Michael N. Schmitt (ed) Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence (Cambridge University Press 2013), 258, referring to this notion as “cyber warfare”.

Electronic copy available at: https://ssrn.com/abstract=3575755
networks by means of cyber capabilities”. This rather specific and enemy centric definition refers to three key criteria:
- the presence of a military operation aimed at achieving a political or military advantage,
- the causing of damage to the opponent’s [sic] cyber infrastructure; and
- the use of cyber capabilities (since computer systems can also be destroyed using kinetic capabilities).

The UK based Chatham House steers away from this enemy-centric definition and applies a more liberal – at least from a legal and law of armed conflict point of view – characterization, concluding that “cyber warfare [sic] can enable actors to achieve their political and strategic goals without the need for armed conflict”.

Taking note of contemporary military doctrine, the military – alongside economic power, diplomatic power and information – are comprehensively used as one of the instruments of state powers to achieve goals by influencing actors through the application (or threat) of ‘fighting power’. Hence, the actors to be influenced could be opponents or enemies, however, neutral actors will be encouraged to stay (at least) neutral or even persuaded to partner with the military, whilst supportive actors will be stimulated to remain supportive. The military is thus instrumental to the state’s strategic interests and goals, providing for a number of strategic functions: anticipation, prevention, deterrence, protection, intervention, stabilisation, and normalisation.

In conclusion, cyber operations are characterized by the employment of cyber capabilities with the primary purpose of achieving military objectives by influencing actors in or by the use of cyberspace.

108 AIV and CAVV, 9, also using “cyber warfare”.
109 ibid, 9.
110 Paul Cornish and others, ‘On Cyber Warfare’ Chatham House <http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf> accessed 1 January 2012, 37, preceded by a definition: “Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target”.
113 E.g. Ministerie van Defensie, Netherlands Defence Doctrine (<http://www.defensienl/binaries/defensie/documenten/publicaties/2013/11/20/defence-doctrine-en/defensie-doctrine_enpdf> accessed 16 March 2014, 2013), 37. In a similar way: US Department of Defense, Doctrine for the Armed Forces of the United States (Joint Publication 1) (25-3-2013 edn, Joint Chiefs of Staff 2013), I–10 – I–11. UK Ministry of Defence, 1–8 – 1–11 – quoting Field Marshal Viscount Alanbrooke – uses the term Military Strategy, being the “art to derive from the [policy] aim a series of military objectives to be achieved: to assess these objectives as to the military requirements they create, and the pre-conditions which the achievement of each is likely to necessitate: to measure available and potential resources against the requirements and to chart from this process a coherent pattern of priorities and a rational course of action”.

Electronic copy available at: https://ssrn.com/abstract=3575755
The military operations paradigm in kinetic and cyber situations alike, provides an institutional framework guaranteeing social legitimacy (public support), as well as legal legitimacy or legality: a proper legal basis to launch operations and adherence to the applicable legal regimes for the conduct of operations. As in any other military operation, an ‘adequate’ legal basis is required before it is decided upon and undertaken. regimes refer to those rules that are applicable once an operation commences. One could think of the law of armed conflict (hereafter: LOAC), human rights law, and military codes. In addition, though they don’t qualify as ‘law’ proper, operational and political guidelines governing the use of force, known as Rules of Engagement (ROE), national caveats, or Tactical Directives et al are considered to be part of the ‘legal regimes’. Both legal bases and legal regimes make up the legal framework for military cyber operations, covering the whole spectrum of (pro-)active, passive, offensive and defensive cyber operation.

5. Response mechanism

The five core paradigms mentioned above – coordination and governance, protection, law enforcement, intelligence and military operations – all have different and unique legal and institutional frameworks, and aim for different effects to be achieved. But on the other hand, the paradigms do overlap, especially in the means and methods used and it must not be excluded that a government agency can operate in different paradigm under different legal coverage.

Furthering and protecting vital interests is not a one-way activity. Rivalling or opposing actors or audiences can take the initiative to act or can react to earlier engagements. Moreover, the cyber security paradigms can have a reactive, proactive or active stance. Democratic societies usually respond proportionally but that does not mean in kind or from within the same paradigm.

---

114 The UK and Dutch doctrines use ‘legitimacy’ as an overarching framework: UK Ministry of Defence, 1–22, “Legitimacy encompasses the legal, moral, political, diplomatic and ethical propriety of the conduct of military force”; and Ministerie van Defensie, 99, “Legitimacy has a legal and an ethical side. Legal legitimacy primarily requires a legal basis for the mission. Secondly, legitimacy is based on the observance of rules that apply during the mission”.


116 This is normally a prerogative of the Executive branch, see: Sascha Hardt, Luc Verhey and Wytze van der Woude (eds), Parliaments and Military Missions (Europa Law Publishing 2012) and Nolte.

117 Legal basis and legal regimes are covered by the denominator of ‘legality’: UK Ministry of Defence, 1–22.


119 Some LOAC rules even apply before operations are launched: e.g. regarding the dissemination of LOAC and the employment of legal advisors.

120 Ducheine and others (n 60) 112.
The most common legal bases for responses are retorsion, countermeasures, a plea of necessity and self-defence.\[121\]

In responding to a prior engagement, the utility of the paradigms is comprehensive within but also beyond cyberspace. An intrusive cyber operation breaching the sovereignty of a state can be answered with diplomatic means or with a hack-back by the protectors supported by a law enforcement legal base. A cyber armed attack can be retaliated with the use of force, both with cyber- but also kinetic means.

Cyber operations, whether initiated by the state, or in response to a prior engagement follow a certain sequence which will be described in section 6.

6. Operationalizing Cyber Operations

As was evident from the description, the paradigms on the state level share many similarities related to common skills, knowledge and techniques, capacities, capabilities in other words in means and methods. Notwithstanding the obvious difference in objectives and its effects, a common model to (describe and thus) operationalize cyber operations is available. This descriptive six-phased model is useful in explaining the modus operandi of (a number of) cyber operations.\[122\]

Though the model itself may be helpful to understand cyber operations in general, it remains crucial to realize that the designated paradigm is of influence for the objectives of the operations defined, and thus for the effects that are to be achieved through these operations.\[123\] The model comprises six phases that – in full or in part – may characterize and describe a typical cyber operation:\[124\]

---


123 To some extent, activities and actors that haven’t received detailed attention so far, e.g. cybercrime/criminals or hacktivism/hacktivists, ‘follow’ this model as well.

• reconnaissance,
• design,
• intrusion,
• action,
• camouflage, and
• exfiltration.

Subject to the particular purpose of the operation, one of more of the phases can be expected. During an intelligence operation with the objective to scan the infrastructure of other actors, an initial operation may be limited to scanning ports, thus the operations will have one phase only: reconnaissance. With the information thus gathered, a more targeted operation may be designed to gather additional information on the hardware and software configuration of the actor’s ICT system, encompassing all phases, with again an intelligence objective. Based on the collected information (taken together with other sources) a supplementary law enforcement operation could be started to gather forensic evidence, again going through all of the six phases. In addition, as a spin-off of the two operations, a designated military operation could be drafted as well, again using one of more of the phases described.

It will be evident that these three examples will be governed by their respective paradigmatic framework, including the legal frameworks. All three operations, will require a legal basis, an objective (end), will need means (operators and tools), and will use methods requiring a plan, an addressee (or ‘target’), techniques tactics and skills, all in accordance with the applicable legal regimes, and have oversight mechanism ensuring legitimacy and accountability. For military operations, these elements are not fully covered by military doctrine (yet). Without going into details, these rather ‘novel’ operations are therefore briefly described below.

7. Operationalizing Military Cyber Operations

The military instrument of power will be used to achieve strategic objectives (of various kinds). Whether employed unilaterally or in a comprehensive manner together with other instruments of power, the military plans and executes operations to influence other actors. Obviously, these actors may be opposing forces, but more generically, these actors may also be friendly/supportive or neutral actors and audiences.

For references, see Joint Doctrine Publications of various states, e.g. NL Ministerie van Defensie; US Department of Defense; and UK Ministry of Defence. For a detailed analysis: Duchêne and Haaster, ‘Fighting Power, Targeting and Cyber Operations’.

125 In general, this also holds true for cyber activities with a hacktivist or criminal purpose.

Through military operations, designed to achieve designated effects for strategic objectives, other actors are affected by alterations in their sources of power, either disruptively or constructively. Military operations – including cyber operations – will be directed ‘against’ the fighting power of another actor in order to achieve these effects.

The traditional addressees or ‘targets’ of these operations may be found in the physical (personnel, tangible objects, materiel and infrastructure) or in the virtual dimension. The latter comprises the psyche of personnel and information in general. By supporting actors with training, equipment or information, the physical, moral and conceptual component of their fighting power will increase, whereas attacking personnel, objects and manipulating information will decrease the (coherence between the) components of fighting power.

Cyber operations on the other hand, will make use of cyberspace comprising the physical network layer (i.e. the hardware) and two layers representing virtual elements: cyber identities and cyber objects.\(^\text{128}\) Firstly, the cyber persona layer contains cyber identities, i.e. the virtual reflection of persons, e.g. e-mail addresses, Facebook-accounts etcetera. Secondly, the logical network layer contains what could be called cyber objects (as a contrast to tangible objects in the physical dimension), e.g. applications (software or code) and data (stored or in process).

The uniqueness of cyber operations lies in the fact that the virtual dimension (as in Information Operations) offers new opportunities to influence actors. By addressing (or targeting) the cyber persona layer (i.e. cyber identities) and the logical network layer (i.e. cyber objects), disruptive and constructive effects can be achieved through cyber operations.

Conceptually, although thorny questions have been brought up and will remain to be addressed, the operational processes for physical or kinetic military operations and cyber

---

128 See supra note 5 for a brief characterization of cyberspace.
operations are alike. This is also the case for the military process called ‘targeting’,\textsuperscript{129} through which objectives are defined, potential targets selected, the available means are listed and evaluated in view of effectiveness and collateral consequences, the means are designated and prepared, and the action is executed and evaluated.\textsuperscript{130}

Evidently, this brief conceptual description of military cyber operations offered is not unique for the military paradigm, as its operationalization can be used in others as well by analogy. What remains exclusive, though, for military cyber operations executed by states, is the paradigm and the (legal) framework that is authorising and governing these activities. Unlike other paradigm, the (strategic) objectives defined are the most far reaching (or extreme) in its ends, means and effects.

8. Conclusion

This chapter set out to elaborate on the phenomenon of what is often coined as cyber operations as a common denominator for cyber activities. After having analysed differences in strategic or ‘corporate’ objectives (for states and non-states alike), the similarities in terms of means to achieve those objects and the ways to employ those means on the operational level (of states and non-state actors) were considered. Moreover, five distinct paradigms are used to shape cyber activities on the state level. The core paradigms – in particular law enforcement, intelligence and military operations - provide the legal basis for governmental powers that may interfere with human rights and privileges. Military operations within the paradigm of conflict represents the most far-reaching framework for governmental action.

Having said that, it is noteworthy however, that cyberspace and its actors are influenced by military jargon (at least). Notwithstanding the idiom used – think of attacks, targeting, cyberwar – the majority of cyber activities are of a non-military nature. Once and again, it appears that the main actors in cyberspace are intelligence agencies (governmental) or enterprises (corporate), and criminals (varying from individual to organised crime), and that the main objectives for cyber operations characterise as sabotage, espionage, subversion,\textsuperscript{131} and crime!

\textit{11400 words text (abstract and table excluded)}

\textit{4700 words footnotes.}


\textsuperscript{131} See National Cyber Security Centre, \textit{Cyber Security Assessment Netherlands (CSAN)-3} and Thomas Rid, ‘Cyber War Will Not Take Place’ 35 Journal of Strategic Studies 5.
Bibliography

- Arquilla J, ‘Cyberwar Is Already Upon Us - But can it be controlled?’ (Foreign Policy, 2012) http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us#sthash.OfFAFk4W.dpbs.
- Australian Attorney-General’s Department, Cyber Security Strategy (http://wwwaggovau/RightsAndProtections/CyberSecurity/Pages/defaultaspx).

26

Electronic copy available at: https://ssrn.com/abstract=3575755

• Convention on Cybercrime.

• DeNardis L, The Global War for Internet Governance (Yale University Press 2014)


• Ducheine PAL and van Haaster J, ‘Cyber-operaties en militair vermogen’ 182 Militaire Spectator 368.


• Ducheine PAL and Pouw EH, ‘Controlling the Use of Force: Legal Regimes’ in Meulen Jvd and others (eds), Mission Uruzgan: Collaborating in multiple coalitions for Afghanistan (Amsterdam University Press 2012).

• Ducheine PAL and Pouw EH, ‘Legitimizing the Use of Force: Legal Bases for Operation Enduring Freedom and ISAF’ in Meulen Jvd and others (eds), Mission Uruzgan: Collaborating in multiple coalitions for Afghanistan (Amsterdam University Press 2012).


• Electronic Frontier Foundation, ‘CISPA is Back: FAQ on What it is and Why it's Still Dangerous’ https://www.eff.org/cybersecurity-bill-faq.


• Ernst & Young, Under cyber attack - EY’s Global InformationSecurity Survey 2013 (Ernst & Young 2013).


• EU Cyber Direct, ‘Cyber Diplomacy in the European Union’ (2019)


• Freedman L, Strategy - A History (Hb edn, Oxford University Press 2013).


• Ginkel B van, Putten F-P van der and Molenaar W, State or Private Protection against Maritime Piracy? A Dutch Perspective (Clingendael Centre for International Relations 2013).


• Hanspach M and Goetz M, ‘On Covert Acoustical Mesh Networks in Air’ 8 Journal of Communications 758.


• ———, ‘Far More than 87m Facebook Users Had Data Compromised, MPs Told | UK News | The Guardian’ (The Guardian, 2018) https://www.theguardian.com/uk-


- Janczewski IJ and Colarik AM, Cyber Warfare and Cyber Terrorism (Information Science Reference 2008).


- Jordan D and others, Understanding Modern Warfare (CUP 2008).


Ministere de 'Europe et de Affaires Etrangeres, ‘Stratégie Internationale de La France Pour Le Numérique’.


Neumann PR and Smith MLR, ‘Strategic terrorism: the framework and its fallacies’ in Mahnken TG and Maiolo JA (eds), Strategic Studies - A Reader (Routledge 2008).


threats-sparke-snooping-fears/#787cc72a5025.

• United Nations General Assembly, ‘The right to privacy in the digital age (UN Doc. GA/11475)’ (2013, 19 December)
• US Department of Defense, *Doctrine for the Armed Forces of the United States (Joint Publication 1)* (25-3-2013 edn, Joint Chiefs of Staff 2013).