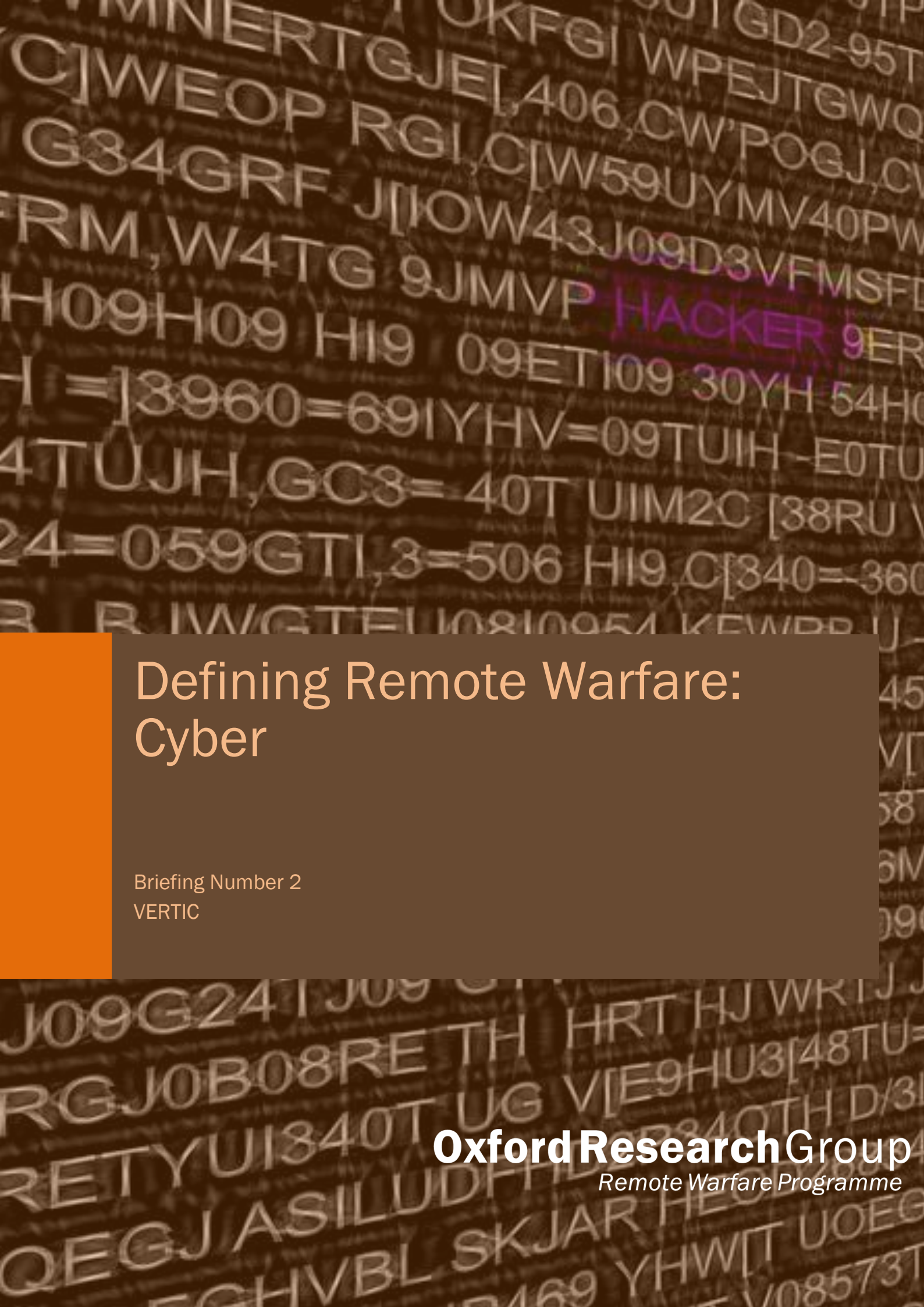

Defining Remote Warfare: Cyber

Briefing Number 2

VERTIC

Oxford Research Group
Remote Warfare Programme

This report has been commissioned by the **Remote Warfare Programme**, a programme of Oxford Research Group. The programme examines changes in military engagement, with a focus on remote warfare. This form of intervention takes place behind the scenes or at a distance rather than on a traditional battlefield, often through drone strikes and air strikes from above, with Special Forces, intelligence agencies, private contractors, and military training teams on the ground.

Published by Remote Warfare Programme, January 2018
Remote Warfare Programme
Oxford Research Group
Development House
56-64 Leonard Street
London EC2A 4LT
United Kingdom
+44 (0)207 549 0298

info@remotecontrolproject.org

http://remotecontrolproject.org

Cover image: Pixabay (The Digital Artist)

About the Series

The *Remote Warfare Programme* is a research and policy unit analysing the rise of remote warfare: the recent shift away from "boots on the ground" deployments towards light-footprint military interventions abroad.

Among other factors, austerity, budget cuts, war-weariness, and high political risk aversion in the wake of Iraq and Afghanistan have all played their part in making large-scale UK military deployments less palatable to the UK Parliament and public.[1]

Alongside this, trends in military engagement such as the increasing use of drones and an increased focus on counterterrorism and building local capacity – evident in, for example, the addition of defence engagement as a core task of the Ministry of Defence – have allowed the UK to play a role in countering threats posed by groups like Islamic State, Boko Haram, al-Qaeda and Al-Shabaab without deploying large numbers of its own troops.

The emergence of approaches that seek to counter threats at a distance, without the deployment of large military forces, is an umbrella definition of remote warfare. With local troops engaged in the bulk of the frontline fighting, the UK's role has, by and large, been a supporting one, providing training and equipment and, where necessary, providing air and intelligence support, and the assistance of UK Special Forces to bolster local troops.

The focus of the *Remote Warfare Programme's* work has been on a strategic level, asking what the implications of these changes in military engagement are for the transparency, accountability and effectiveness of UK military engagement abroad.[2]

However, to ask these strategic questions, we have often had to put to one side the fact that remote warfare is not an uncontested term, and our broad definitions and analysis often hinge on an assumption that "you know it when you see it". Moreover, while we have been focusing on the use of remote warfare on today's battlefield, we are also aware that future changes in technology, especially the rising importance of cyber and autonomous weapons, will have an impact on how we should understand remote warfare.

This series brings together experts to discuss important aspects of remote warfare to provide some conceptual clarity. It looks at current practice, including reports on security cooperation, intelligence sharing, private security companies and drones, as well as looking to the future of warfare: addressing how offensive cyber operations and autonomous weapons could change the landscape of military engagement.

Over the course of the next year, we will release bi-monthly briefings on these subjects by experts in their field, with the eventual aim of exploring common themes, risks and opportunities presented by the evolving use of remote warfare.

About this briefing

As the capacity of the internet grows and its presence proliferates, its potential as a military tool evolves. Pushing far beyond traditional uses of cyber for things like communication, militaries are now beginning to consider cyber as a military domain, with the potential to exploit networked assets and use internet-based attacks in addition to or instead of their use of conventional weapons.

Looking to military doctrine of the UN Security Council's Permanent Five (P5), it is clear that all of these states agree that cyber events are increasing in prominence. There is also agreement that these operations have military consequences. However, there remains a large amount of ambiguity as to how these tools will be used – and how other governments and militaries will interpret such use. Additionally, there is currently no clear definition of what constitutes cyber war.

Even defining the concept of "cyber" comes with complications. For the purposes of this paper, cyber is defined as any form of networked communications, or computer assets, used by a state or non-state actor. Cyber-attacks are defined as using malicious code to negatively interfere or surveil a system. If apparently hostile cyber activities are detected, contrasting points of view between states on what constitutes cyber warfare could result in the unnecessary escalation of tensions.

Challenges in conclusively attributing the origins of these activities can increase uncertainty about others' intentions and actions, altering calculations about how best to respond. The use of cyber-attacks also threatens the security of the internet for civilian use and raises the possibility of civilian infrastructure like power plants, water utilities and air traffic control, being directly or indirectly targeted. Without greater clarity over what sort of attacks will elicit an aggressive response the deterrent ability of cyber capabilities will be eroded, the risk of states misreading each other is heightened, and the cyber age may increase global instability.

Author

VERTIC is an independent, not-for-profit non-governmental organisation. Our mission is to support the development, implementation and effectiveness of international agreements and related regional and national initiatives, with particular attention to issues of monitoring, review, legislation and verification.

VERTIC publishes its research on verification regimes through a series of openly available publications. The centre also offers training through workshops carried out around the world, as well as through our internship programme. We help governments and international organisations in their efforts to make regimes binding by offering ratification support. VERTIC also assists governments in translating commitments undertaken in international law into national legislation and regulation. We conduct all our work in an objective and impartial manner.

Contents

Introduction

Cyberwar has grabbed the attention, and imagination, of publics, media, civil society and academics alike. On one hand, cyber-related news is an increasingly common fixture in mainstream outlets, with stories of potential cyber-attacks and Russian interference in foreign elections making easy click bait; while on the other, many universities and research institutes have been developing their own cyber research departments.

Moreover, states are seeing cyber as an increasingly important part of their military strategy. For example, the UK Government declared in its 2015 Strategic Defence and Security Review that cyber-attacks represented a vital threat to the UK and promised to remain "a world leader in cyber security."[3] More recently, President Trump elevated Cyber Command, the Pentagon's offensive cyber-force, to make it its own unified military command "in a move that is meant to strengthen cyberspace operations and bolster U.S. defenses."[4]

"[C]yberwar appears to represent a clear example of remote warfare where states can engage in offensive operations against other states without having to deploy large numbers of their own troops to the frontlines, often in complete secret"

In many respects, cyberwar appears to represent a clear example of remote warfare where states can engage in offensive operations against other states without having to deploy large numbers of their own troops to the frontlines, often in complete secret and with a much lower prospect of their responsibility being revealed.

However, despite the furore surrounding it, cyberwar remains a much discussed yet little understood issue. As this report notes, the concept of cyberwar remains nebulous and offensive cyber operations often appear to amount more to "cyber-vandalism" than traditionally understood military operations. Moreover, beyond some public statements, national policies remain heavily classified and vague commitments to prioritise cyber tell us little about how cyber will be incorporated into national defence strategies.

This report adds to the debate by investigating how cyber could fit into traditional understandings of military doctrine and strategy, and therefore how it might fit in with the *Remote Warfare Programme's* work on changes in military engagement. First, it lays out the definitional issues of seeing offensive cyber operations as part of traditional understandings of war and conflict by giving an insight into the conceptual difficulties governments and academics will face when trying to comprehend cyberwar.

Second, it describes how the military doctrine of the UN Security Council's Permanent Five (P5) – the US, the UK, France, China and Russia – have begun to include cyber. This gives some insight into how some of the most militarily influential countries in the world perceive cyber in respect to their military strategy and draws out some common trends and distinctions between the five nations.

Finally, the report looks at the ways in which cyber could be incorporated into

military strategies by applying it to the concept of deterrence. As we shall see, two key properties of cyber warfare – the difficulty that it poses to efforts to attribute attacks to specific state or non-state groups and the speed and breadth of developments in the cyber sphere – pose governments with a series of problems when it comes to using these capabilities. This ambiguity – which is worsened by the lack of clear and transparent guidance on what cyber warfare means to different states – increases the risk of unwanted and unwarranted escalation of conflicts from the cyber to the physical realm.

Methodology

This briefing will discuss the treatment of cyber in the current doctrine of P5 states and then examines the opportunities and barriers posed by the integration of cyber capabilities into national deterrence strategies.

Military doctrine is an important indicator of the way that states view, integrate and use both established and new technologies in security planning, posture and operations. Comparing countries' military doctrine can therefore provide a picture of the convergence or divergence in interpretations of the cyber domain between governments and highlight where any lack of clarity or agreed positions may heighten escalation risks. The doctrine of the members of the UN Security Council have been chosen as these countries have disproportionate influence over UN decision-making for security issues and each holds a veto over UN-sanctioned military action. This paper assumes that the doctrine from these states' militaries will influence other states' policies, and therefore provide a good starting point for considering cyber-military issues. Furthermore, these states are among the most advanced in terms of cyber defensive and offensive capabilities, and thereby show the likely 'direction of travel' in international cyber security affairs.

Although it is clear that countries are ramping up their cyber assets, states have been reticent to provide specifics on what they plan to do with these resources. States have been willing, however, to broadcast their cyber readiness in their military doctrine, which may have an important deterrent function. For this reason, we have chosen to examine the opportunities and barriers posed by the integration of cyber capabilities into national deterrence strategies.

Cyber-attacks or cyber warfare?

Cyber warfare is victim to mis-definition and is a widely misunderstood, burgeoning form of conflict. The rapidly changing character of war further adds to the challenge of finding a succinct definition for cyber warfare. However, at a fundamental level, most known cyber-attacks to date have had a similar format: outwardly aggressive but with few lasting results. For example, the North Korean hack of Sony in December 2014 leaked personal information, emails and unreleased films, causing humiliation for Sony staff and a large expense.[5] Ultimately, though, President Obama labelled it an act of "cyber vandalism". This was an observant comment, as many cyber-attacks resemble acts of sabotage or vandalism because they disrupt or damage a system or interface temporarily.[6] Further, it would have been deemed disproportionate for Obama to respond with force to an act of vandalism. An act of war, involving or threatening a

large loss of life, would be considered to require a national response, either in kind – cyber or kinetic.

Whether a cyber act can be an act of war, is often debated by policy makers and cyber experts alike. King's College London professor Thomas Rid argues that cyber acts are not acts of war, at least in a traditional sense, in his book *Cyber War Will Not Take Place*. Rid demonstrates the shortcomings of a defining a cyber act as an act of war concisely: "If the use of force in war is violent, instrumental, and political, then there is no cyber offense that meets all three criteria."[7] Singer and Friedman, authors of the book *Cybersecurity and Cyberwar: What You Need to Know,* advocate similarly: "war always has a political goal and mode (which distinguishes it from crime) and always has an element of violence."[8]

"[C]yber-attacks may be used as part of a spectrum of remote warfare capabilities, which seek to use military means other than the deployment of large numbers of boots on the ground to achieve strategic objectives."

Despite differing understandings, some recent events could be construed as instances of cyber warfare which, if designed with different outcomes, could meet Rid or Singer and Friedmann's criteria. Stuxnet is frequently cited as an example of an attack targeting national infrastructure, which is a common tactic during warfare. The primary aim of Stuxnet was to cut Iranian uranium production, which was achieved by running a malicious code to speed up the spinning of the centrifuges and eventually caused them to self-destruct.[9] The assailants planned for the attack to go undetected: any damage was designed to appear as an error and cause engineers to put the project on hold.[10] If the attack on the centrifuges had caused more violent results, the response by the Iranian government might have been different. For example, if the centrifuges had been coded to explode and cause a fire, not only destroying the facility but also harming staff, it is fair to assume that the Iranian government would be pushed to uncover the cause of the incident and follow through with a proportional response.

Some evidence suggests that Iran did follow through with a response some time later, in the form of the 2012 attack on Saudi Aramco, causing 35,000 computers within the oil company to be taken down and deeply effecting distribution.[11] This attack, while devastating to the company's operations, had limited physical consequences.

However, this begs a number of questions, such as: What happens if a more violent Stuxnet occurs? Will the affected nation strike back? Will they respond with a cyber-based attack or launch a more kinetic form of war? This confusion has caused many prominent cyber security experts and scholars to ask, where does cyber vandalism end and cyber warfare begin? When does a cyber-attack become an act of war?

What is truly new about cyber warfare?

In addition to the ambiguity regarding when cyber-attacks become acts of war, the character of modern warfare is challenging the existing idea of an act of war. Formal declarations of war have become increasingly rare. The US, for

example, has not formally declared war since 1942.[12] Instead, the separation of states of war from conditions of peace are often blurred, and all-out war between states is an increasingly rare phenomenon.

In modern combat, cyber-attacks may be used as part of a spectrum of remote warfare capabilities, which seek to use military means other than the deployment of large numbers of boots on the ground to achieve strategic objectives. Conflict can involve opponents with vastly different capabilities: a gifted group of hackers, for example, could have as much impact on military communication as an opposing military.

However, it is also clear that the use of cyber-attacks does not necessarily mean that we are entering a new era of warfare. Cyber-attacks can be employed alongside the panoply of other "hard power" tools that a state may use. The UK defines "hard power" as military or economic activity that aims to "coerce opponents to adopt a particular course of action."[13]

Indeed, while cyber might represent a different means of achieving an end, the ends that it can achieve can be similar to those achieved through conventional force. Then Prime Minister of Estonia, Andrus Ansip, compared the extensive distributed denial of service (DDoS) attacks (which flood a website with users to render it temporarily unusable) on government sites to a blockade of a port.[14] Like a blockade of a port, the DDoS attacks limited the distribution of goods (through limiting financial transactions online) and government activities and communication (through blocking websites and communication portals).

Nevertheless, while the attack caused mass confusion and panic it did not result in escalation or long-term damage, and later was declared as outside the remit of the law of war.[15] Cyber security experts Peter Singer and Alan Friedman acknowledge that it is ultimately the leadership of a state that decides whether a cyber-attack qualifies as an act of war that may be legally responded to with military force.[16] This is where cyber may represent a boost in capabilities for actors who prefer to operate in the "greyzone" between war and peace – a utility that is enhanced by the difficulty that cyber capabilities pose for those attempting to reliably attribute them to specific state or non-state actors.

The ambiguities surrounding the form that a cyber-attack should take in order to elicit a legitimate military response are no doubt designed to give states freedom of manoeuvre, as it creates uncertainty that in turn makes it more difficult for an opponent to exploit thresholds by consistently operating just underneath them. However, as we shall see in the following sections of this report, this uncertainty also enhances the risk of misunderstanding or miscalculation, which may weaken the deterrence function of cyber and raise the risks of unwanted or unwarranted escalation.

What we can tell about cyber from P5 doctrine

Military doctrine is a strong medium through which to explore current military thinking, and how cyber is being considered as both a vulnerability and a capability. Indeed, the very appearance of cyber initiatives within doctrine suggests that cyber forces may have finally arrived. Conceptually, doctrine answers the question of what a state plans to do with

Barack Obama chairs a United Nations Security Council meeting (image: Wikimedia Commons, 2009)

its security-dedicated resources – a major question provoked by the substantial cyber budgets currently being published.[17] Many aspects of military doctrine are precise and refer to technical issues of command and control, yet doctrine also operates as a philosophical touch-point for a military both in times of peace and war. The UK, in its 2010 Army Doctrine Publication, states that the doctrine contains "the enduring philosophy and principles for our approach to operations."[18] Doctrine also allows a state to express their moral obligations in war, and how they believe military action can relate to greater statecraft.

Military doctrine also reveals how states think cyber issues will play out on the international stage. Through well-crafted doctrine, a state can reveal or obscure internal struggles while projecting military power and aggression to allies and enemies alike. For example, in their 2010 doctrine, Russia signalled a reduced threat of nuclear use through a language alteration, changing the wording from "in situations critical to the national security" to situations where "the very existence of the state is under threat."[19] Doctrine, therefore, will be a key area for states to broadcast the readiness of their cyber defences and their capacity for offensive cyber operations.

Ultimately, the drafting of military doctrine is preparation for preventing and fighting future wars. Therefore, predicting how technology will alter the battlefield has been a main objective of doctrinal development. For example, technological advances such as drones have transformed reconnaissance and strike missions for the UK Military: a briefing paper by the House of Commons notes that drones can give ground forces a near constant visual of the movement of enemy forces. On the other hand, it is recognised that drones are highly susceptible to network interference and this needs to be considered when deploying them.[20] Even limited cyber activities, when deployed militarily, will have a significant impact on the landscape of future warfare.

United States

The key source for understanding current US doctrine on cyber space is the 2015 Department of Defense Cyber Strategy, which is supplemented by Joint Publication 3-12 R on Cyberspace Operations. The primary goal of the US

cyber military doctrine is to defend its own use of cyber assets, as networked systems have become dominant throughout its branches. The military sees reliance on cyber capabilities as a vulnerability, and in response, has made a large training investment in exercises that simulate operations in conditions with degraded networks. The US expects a high number of adversaries in this field due "to minimal barriers to entry and the potentially high payoff."[21] For this reason, the Department of Defense (DoD) states that defensive exercises form the "vast majority" of the 2015 Cyber Strategy. An overarching goal of the doctrine is to maintain the internet as an open and safe space, as it states that it "will always conduct cyber operations under a doctrine of restraint, as required to protect human lives and to prevent the destruction of property."[22]

From an offensive perspective, the DoD aims to insert cyber operations into its regular spectrum of attacks and synchronize its cyber capabilities across its departments. The DoD believes that most offensive and defensive cyber operations will be joint endeavours between two or more branches of the military (*3-12 R*, I-6). As far as offensive cyber operations are concerned, the American military has three primary goals: to "degrade, disrupt or destroy" other cyber-based communications and infrastructure.[23] In spite of large investment and planning in this field, the US admits to limitations in cyberspace - like an undeveloped command and control function.[24]

The US may not have a specific definition a cyber act of war, but they have made efforts to clarify what types of disruption do not qualify: "defacing a government webpage; a minor, brief disruption of internet services; briefly disrupting, disabling, or interfering with communications; and disseminating propaganda."[25]

United Kingdom

Unlike the US, the UK does not have a separate, public cyber strategy document. Instead they include cyber aspects in their comprehensive military doctrine (produced by the joint staff) and other areas of governmental documentation. The UK's dedicated "Cyber Strategy" encompasses some military concerns but is published by the Cabinet Office (the supporting governmental branch of the Prime Minister). These differences in approach reflect the way in which cyber issues now permeate every branch of government and society, opening possibilities for varying interpretations of how to manage the technology and its impacts.

The strategy's three main tenets are to "Defend, Deter and Develop". Defense refers to identifying and maintaining systems to defend the UK's cyber architecture. Deter means that the UK plans to bolster its cyber security and strategy to deter attacks using cyber techniques. The UK remains ambiguous as to what these techniques are and how exactly they will bolster said strategy. Develop, finally, refers to building UK infrastructure and education to ensure a thriving private sector and new generation of experts. [26]

The UK asserts that a primary goal of cyber security strategy should be the maintenance of the internet as a safe place. However, they do advocate that offensive cyber strategies should be developed.[27]

France

Military-based cyber activities were first publicly mentioned in the 2008 edition of "The White Paper on Defence and National Security". Like the US, France acknowledges that a growing public and military reliance on networked assets is a vulnerability for the state. However, the White Paper refers only to their cyber policy as a cyber-defence policy, suggesting that offensive operations are secondary, non-existent or undeclared.

The 2013 edition of the White Paper builds upon the previous edition and identifies areas to strengthen, as it believes that cyber vulnerabilities will become more prevalent. The paper notes that cyber-attacks "do not have the same impact as terrorist acts, given that they have not to date resulted in any fatalities. However, today and even more over the timeframe of this White Paper, they represent a major risk given their high probability and potential impact". It adds that "Large quantities of information of great strategic, industrial, economic or financial value are stolen, often unbeknownst to the victims. The recurrence of this type of infiltration today, notably on the part of States, could suggest that information is being methodically collected to facilitate a large-scale attack in a conflict situation. Such an attack could easily paralyse whole swathes of a country's activity, trigger technological or ecological disasters and claim numerous victims. It could therefore constitute a genuine act of war."[28]

The paper also emphasizes a close relationship with other European powers. In particular, sensitive issues are shared and approached in unison with the UK.[29] The White Paper recognizes the growing use of "offensive IT capabilities"[30] and suggests that key allies like the US will be more likely to engage in targeted attacks carried out by special forces that may be "cybernetic" in capacity.[31]

China

The Chinese Academy of Military Sciences publishes a document called the *The Science of Military Strategy* roughly every fifteen years, which details the evolution and goals for Chinese Strategy.[32] Experts have read and commented on the most recent theoretical strategic plans, released in 2013. In contrast to previous manifestations, the newest edition contains an entire chapter on cyber war and contains details on "network reconnaissance, network defence, network attack and network deterrence."[33]

The Chinese, *The Diplomat* reports, aim to take a "whole nation" approach, which will allow for senior military staff to mobilise the skill-set of both civilian hackers and private sector experts.[34] The first step to achieve this "whole nation" approach is an integrated structure to cyber warfare, building cyber warfare units into the military, other government ministries and non-governmental forces (presumably contracted groups).[35]

China sees cyber weapons as an important tool for manipulating and controlling the information of its adversaries, inside and outside of their borders.[36] Domestically, China is particularly concerned with the potential for the internet to be used as a platform of expression for political dissidents. On several occasions, China has been accused of launching cyber-attacks against its own populace – most recently to censor access to social media during the protests in Hong Kong. Large distributed denial of

service attacks (DDoS) were enacted against two independent media outlets, to stem traffic to the sites.[37] China is also particularly concerned with the amount of Western ownership of cyberspace, referring to it as "network hegemony."[38] China sees their "main strategic opponent" as the US, and fears that the country has superior network warfare abilities.[39]

Russia

Currently, the available doctrinal document for Russian military activity in cyberspace is called "Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space", which was published in 2011.

Circulation of information is a major concern for Russia. As stated in their "Conceptual Views", Russia is most concerned with the "threat of the use of content for influence on the social-humanitarian sphere".[40] Russia's Institute of Information Security Issues (IISI) fears other states, particularly the US's ability to facilitate and manage protests through information superiority.[41] Russia also has a different conceptualisation of state sovereignty over the internet resources in its own territory to Western states like the US, UK and France.[42] For these reasons, information security and control of the media are closely tied.[43]

Common Trends

All states have recognized the growing relevance of cyber space to national security and believe that it requires a serious and integrated strategy across both military and government. Every military doctrine reviewed suggests a joint approach, either between several branches of the military and/or a combination of government and military activities. Within these approaches, the emphasis is currently on defensive capabilities, but with indications of a growing focus on offensive capabilities as well.

Nevertheless, there are other aspects of cyber warfare that are not approached with such uniformity, and different countries have developed approaches that reflect other aspects of their foreign or domestic politics.

"All states have recognized the growing relevance of cyber space to national security, and believe that it requires a serious and integrated strategy across both military and government."

For example, there is an oft-noted divide between the US and Europe, and China and Russia. Sebastian Bae, a cyber warfare expert, argues that China and Russia have chosen information warfare – in the form of distributing propaganda and the control of internal communications – as opposed to the weaponisation of cyber means. Bae suggests that their objective of manipulating and controlling information will ultimately be more successful than other states that are more focused on network damage or disrupting communications (like the US).[44] The US and Europe, however, steer away from this kind of thinking as they are concerned that it will negatively affect freedom of speech and economic prosperity in their countries.

The military doctrines also suggest that for the US, Russia and China, cyber tactics

are seen as an entry point to a much older and fundamental warfare concept: information superiority. In this case, as opposed to information warfare, information means international communications and intelligence, and information superiority means protecting and maintaining a state's own information and communication (intelligence and command and control in most cases), as well as exploiting or compromising their opposing states' information security.[45]

The US, the UK, France and Russia recognize that the law will limit their actions in cyberspace. The US Military has an entire Joint Publication dealing with the legal implications of cyber operations (JP 1-04). However, the doctrines suggest that development of the international legislative side of cyber activities should be improved. Some states call for a greater UN involvement in cyberspace: Russia has said that it would like to conclude an agreement with the UN regarding internationally established rules and norms.[46] France calls for a "more focused international debate" on how to respond to non-state actors in cyberspace, how Article 51 of the UN charter (regarding the inherent right to individual or collective self-defence)[47] applies and the implementation of the Responsibility to Protect.[48]

Cyber capabilities and national deterrence strategies

In international relations, deterrence is when a state attempts to dissuade an adversary from a particular course of action by advertising devastating consequences. From the point of view of the potential attacker, these advertised consequences may increase the cost of taking a certain action, making it less attractive despite the perceived benefits of an attack. In the modern age, much deterrence theory has focused on the role of nuclear weapons both with regard to their own long-range, fast, destructive capabilities and, for some countries, as a means of compensating for inferior conventional forces. There is an on-going scholarly debate as to whether nuclear deterrence is effective, but this paper will use only the assumptions employed by states on this issue: that deterrence is effective and is a centrepiece of their military doctrine.

While all the P5's military doctrine makes some reference to deterrence, only the UK and US mention it in direct relation to cyber.[49] Neither is clear, however, on the blend of defensive and offensive cyber capabilities that may be required to provide an active deterrent.

The UK's Joint Doctrine Publication 0-01, identifies four pillars of deterrence "credibility; communication; comprehension; capability" (*JDP 0-01,* 64), which provide a strong structure for understanding how deterrence works. These will be discussed in more depth, below, and their use in cyber activities is considered.

Credibility and Capability

Credibility means that a potential attacker believes that the opposing state is both capable of acting upon their advertised consequences for a specific action or "threat", and that it is likely they will. If a capable state makes a threat it can credibly act on, it is considered more likely that the threatened state will not take the undesired action. Conversely, a deterrent message given with low credibility will most likely have a very small impact on the behaviour of its intended targets.

China, for example, is a state that has demonstrated its credibility and capability in the cyber realm. The *New York Times* hack at the end of 2012 is thought by some to have revealed the extent of the Chinese cyber-attack apparatus within their military. After initially intruding the *Times* computer network, the hackers were able to track the journalists' movements for four months, and install malware to allow for continual re-entry into the systems. It is reported that because the attack began while the *Times* was working on an article about the then-Prime Minister's family, it suggests that the People's Liberation Army was attempting to suppress the story.[50] In the framework of deterrence, this incident could be seen as demonstrating China's credible ability to carry out an advanced cyber-attack.

Credibility in the non-cyber realm may also aid to deter cyber-attacks. The US asserts that if attacked with a strong enough cyber-attack, the military would be forced to respond with a conventional armed attack in order to maintain their deterrent posture. Therefore, the US's willingness to utilize their military superiority in other realms during this form of conflict may lend them the credibility to deter cyber-attacks.

The New York Times was hacked in 2012 (image: Flickr: The New York Times Building, 2012)

Credibility is particularly important when applied to the cyber realm, because unlike nuclear weapons or conventional warfare, states cannot easily display or describe what they have in their cyber arsenals. This leaves a limited range of public strategies and events through which to understand states' credibility and capability in the cyber realm, which may pose problems when it comes to the next important pillar of deterrence: communication and comprehension.

Communication and Comprehension

Communication is another crucial aspect of deterrence: states want potential attackers to be aware of the consequences of their actions and to comprehend how the situation may develop. Doctrine and diplomatic posturing are key to communicating a

deterrent threat. It is therefore unsurprising that many states have released national "Cyber Strategies" and have stated at press conferences that cyber capabilities are a primary objective. All the states concerned in this paper have done so in some capacity. As early as 2013, the UK's defence secretary announced that the military would be pursuing an offensive cyber capacity in conjunction with other states.[51] Broadcasting offensive capabilities in military doctrine is a key method to effectively communicate a deterrent force.

Comprehension means that the side issuing the deterrent message has a thorough understanding of which behaviours would effectively cross the red line they are establishing, and the type of response each of these behaviours would warrant. The attacker will not be deterred if they do not believe the advertised consequences will occur at the thresholds that have been communicated to them. Poor communication or comprehension of red lines may lead to unwanted or unwarranted escalation.

Of course, the ambiguities surrounding the form that a cyber-attack should take in order to elicit a legitimate military response are no doubt designed to give states freedom of manoeuvre, as it creates uncertainty that in turn makes it more difficult for an opponent to exploit thresholds by consistently operating just underneath them. However, for cyber capabilities to be an effective deterrent, greater clarity around cyber redlines and definitions of cyber warfare may nonetheless be necessary.

The biggest difference between cyber deterrence and the more traditional understanding of deterrence, relating to nuclear weapons, is that the threshold for use of nuclear weapons is less ambiguous: all nuclear explosions are easy to identify, and any use of nuclear weapons warrants a nuclear response in every nuclear-capable state's doctrine. This makes the price of an attack high and the consequences for the attacker very obvious. Conversely, in the cyber realm, drawing a line is problematic as attacks or intrusions can be extremely difficult to attribute and have a broad range of severity[52] – problems that we will now discuss in more depth.

Why "Cyber-Deterrence" may not work

The attribution question

Attribution, a barrier for many aspects of effective cyber security, is also a barrier for effective deterrence. If an attacker's identity cannot be established with certainty, it severely complicates a state's ability to respond with aggression. The US military theorizes that this anonymity may lead to many more attacks, as cyber provides "a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests" (*DoD Cyber Security Strategy,* 9). Attribution, in many cases, is similar to putting together a puzzle where certain pieces suggest different groups or governments. However, these pieces may not result in a cohesive picture. While identification is possible, it is certainly not assured, and in a best-case scenario the identifier may only have strong confidence in their attribution rather than definitive proof.

To maintain a credible deterrent, states must respond effectively and swiftly to attacks over a certain threshold. However, states that respond to an attack without certainty of the attacker's identity face

huge reputational risk. If a state experienced a devastating attack, leaders may feel the need to attribute and respond quickly, even when there is a lack of evidence. If the attack was attributed to another actor later, the legitimacy of an aggressive response will likely come under severe scrutiny and may raise international tensions. As a result, states are disincentivized to seek retribution after experiencing cyber aggression.

The fast pace of change

Additionally, the capabilities of cyber weapons are constantly changing. While a state may be able to draw a deterrent line for one type of attack, it may be inappropriate for a previously unseen form. The development of norms and laws to govern cyberspace will certainly aid this process, but until then, maintaining a public stance on cybersecurity that is punitive, predictable, yet flexible and responsive to different scenarios, is a major challenge for modern leaders.

This is compounded by the fact that bolstering cyber defences is not necessarily guarantee of decreased vulnerability. With conventional warfare, a state can increase training or investment to counter identified threats. The lack of specificity in cyber-attacks makes a comparison in this area near impossible: the creators of cyber weapons may choose their target and their desired effect, but they have to find a vulnerability to enter a network and carry out the intended attack. However, a cyber-attacker only needs one vulnerability in an adversary's network to infiltrate, meaning, even if a state ramps up cyber defences as a consequence of an advertised threat, it is unlikely that they will be able to stop every gap.

Another limitation is that once threatened, a state can increase their cyber defences and preparedness. These measures may make deterrence less effective: especially if a state increases its cyber-espionage techniques by monitoring another state. For example, the US was apparently able to identify the origins of the Sony attack quickly because the National Security Administration placed "malware that could track the internal workings of many of the computers and networks used by the North's hackers". Once the attack had occurred, they were able to trace back the activity and identify the culprit.[53] It is likely that this form of tracking is common between adversarial states and that once a threat is issued, a state may be able to tap into their espionage network to track and limit their opponent's activities.

As cyber conflict and cyber espionage become more pervasive, it is fair to assume that many states will be under near constant surveillance, potentially easing attribution efforts, but also increasing the risk of unwanted escalation in the case that cyber espionage efforts – which may be conceived of by the initiating state as defensive – are discovered and interpreted as offensive.

Concluding Remarks

Much of this paper has focused on reading states' current postures, and interpreting events through a lens that attempts to understand cyber-attacks within a more established world of military and political strategy.

The doctrine reviewed has demonstrated that while there is some consensus between P5 nations – all states agree that cyber issues are becoming ever more prominent, that there are military consequences of these operations, and that a legal dimension to this issue is missing – there is a large amount of ambiguity as to how these tools will be used and will be interpreted when they are used.

This weakens the utility of cyber capabilities for national deterrence strategies, as the current opacity increases the risks of unwanted and unwarranted escalation. There is a difficult balance to be struck for governments between maintaining ambiguity to increase freedom of manoeuvre, and clearly communicating credible thresholds that can reliably deter the actions of adversaries.

Understanding why a cyber-deterrent may fail should assist military decision makers in creating a stronger deterrent which theoretically, should lead to fewer outbreaks of cyber conflict or escalation. Likewise, abandoning tools that may have too many pitfalls and potential for miscalculation will minimize reliance on poorly developed strategies. As long as the results and efficacy of these strategies remain ambiguous, militaries and governments should approach them with extreme caution.

In creating cyber military doctrine, the states examined have used human resources to apply cyber assets to military strategies. These resources include cyber experts, military decision makers and politicians, amongst others. Maintaining an architecture that is well-informed and responsive to changes in this rapidly advancing field is essential in building military policy that avoids unnecessary conflict.

Finally, policymakers should work at the international level to coordinate responses and understandings of cyber risks and opportunities. Current meetings are slow-going and result in few agreements between states with diametrically opposed understandings of the cyber space, but they provide an essential forum for states to publicise these disagreements. While this debate may not yield substantive results in the near future, such as agreements or treaties, it can assist states in comprehending other states' policies, reducing ambiguity, and reducing the chances of unwanted or unwarranted escalation as a result of a misunderstanding or miscalculation.

Endnotes

[1] Joshi, S. (2015) Future Wars Will Need a More Versatile Response. Retrieved on September 15, 2017, from http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11735180/Future-wars-will-need-a-more-versatile-response.html; Milne, S (2014) A 'Pause' in Centuries of British Wars Is Not Enough. Retrieved November 15, 2017, from https://www.theguardian.com/commentisfree/2014/feb/12/pause-centuries-british-wars-elite-panicking; Economist (2014) Missing in Action. Retrieved November 15, 2017, from http://www.economist.com/news/britain/21598654-britain-needs-strategy-make-best-use-its-shrinking-military-capabilities-it-isnt

[2] Knowles, E., and Abigail Watson, A. (2017). All Quiet On The ISIS Front: British Secret Warfare In The Information Age. Retrieved September 15, 2017, from http://remotecontrolproject.org/publications/quiet-isis-front-british-secret-warfare-information-age/.

[3] UK Government, "National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom" (HM Government, November 2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

[4] Thomas Gibbons-Neff and Ellen Nakashima, "President Trump Announces Move to Elevate Cyber Command," *Washington Post*, August 18, 2017, sec. Checkpoint, https://www.washingtonpost.com/news/checkpoint/wp/2017/08/18/president-trump-announces-move-to-elevate-cyber-command/.

[5] "Timeline: North Korea and the Sony Pictures hack", Lori Grisham. *USA Today,* January 5th 2015. url: http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/

[6] "Obama: North Korea hack 'cyber-vandalism,' not 'act of war'", Sean Sullivan, *The Washington Post*, December 21, 2014. url: http://www.washingtonpost.com/blogs/post-politics/wp/2014/12/21/obama-north-korea-hack-cyber-vandalism-not-act-of-war/

[7] *Cyber War Will Not Take Place,* Thomas Rid. Hurst & Co, London, 2013, 4

[8] *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Friedman, Alan. Singer, P.W.. Oxford University Press, New York, 2014, 121

[9] Sanger, David E.. 'Obama Order Sped Up Wave of Cyberattacks Against Iran', The New York Times, June 1, 2012. url: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&module=Search&mabReward=relbias%3Ar%2C%7B%221%22%3A%22RI%3A5%22%7D&_r=0

[10] Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. Broadway Paperbacks, New York 2013, 188-189

[11] Pagilery, Jose. "The inside story of the biggest hack in history", CNN tech, August 5, 2015. url: http://money.cnn.com/2015/08/05/technology/aramco-hack/

[12] "Hackers Remotely Kill a Jeep on the Highway—With Me in It", Andy Greenberg. *Wired,* July 21st, 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[13] Page 66, Joint Doctrine Publication 0-01, Ministry of Defence. December 8th, 2014. url: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf

[14] Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013), 31.

[15] *The Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press 2013, 75. url: https://ccdcoe.org/tallinn-manual.html

[16] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar What Everyone Needs to Know* (Oxford ; New York: Oxford University Press, Usa, 2014), 126.

[17] *Military Doctrine: A Reference Handbook,* Bert Chapman. Praeger, September 2009, 2
[18] *Army Doctrine Publication,* November 2010. Development, Concepts and Doctrine Center, iii. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33695/ADPOperationsDec10.pdf
[19] Nikolai Sokov, "Why Russia calls a limited nuclear strike "de-escalation"". *The Bulletin of Atomic Scientists,* March 13th, 2014. url: http://thebulletin.org/why-russia-calls-limited-nuclear-strike-de-escalation
[20] "Overview of military drones used by the UK armed forces", *Briefing Paper, Number 06493, 11 September 2015.* Louise Brooke-Holland, House of Commons, 6
[21] "Joint Publication 3-12 R: Cyberspace Operations", Joint Staff, February 2013, II-2. url: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf
[22] The Department of Defense, "The DoD Cyber Strategy," April 2015, 6, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
[23] The Department of Defense, "The DoD Cyber Strategy."
[24]*The DoD Cyber Strategy,* April 201, 5. url: http://www.defense.gov/home/features/2015/0415_cyber--strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
[25] Department of Defense Law of War Manual, Office of General Counsel Department of Defense, June 2015, 1005. url: http://www.defense.gov/pubs/Law-of-War-Manual-June-2015.pdf
[26] "National Cyber Security Strategy 2016-2021", 2016, 9. url: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
[27] "National Cyber Security Strategy 2016 to 2021," *GOV.UK*, November 11, 2016, 51, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.
[28] Page 48. "French White Paper on Defence and National Security", 2013. url: http://www.rpfrance-otan.org/White-Paper-on-defence-and
[29] "White Paper on Defence and National Security," *La France À l'Otan*, April 29, 2013, 21, https://otan.delegfrance.org/White-Paper-on-Defence-and-National-Security.
[30] Ibid., 37.
[31] Ibid., 30.
[32] "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy", Joe McReynolds. *China Brief Volume: 15 Issue: 8,* April 16th, 2015. url: http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=43798#.VdHO-yxVhHw
[33] "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy", Joe McReynolds. *China Brief Volume: 15 Issue: 8,* April 16th, 2015. url: http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=43798#.VdHO-yxVhHw
[34] Joe McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy," *China Brief* 15, no. 8 (April 16, 2015), https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfare-lessons-from-the-science-of-military-strategy/.
[35] Ibid.
[36] Sebastian Bae, "Cyber Warfare: Chinese and Russian Lessons For US Cyber Doctrine", Georgetown Security Studies Review, May 7th, 2015. url: http://georgetownsecuritystudiesreview.org/2015/05/07/cyber-warfare-chinese-and-russian-lessons-for-us-cyber-doctrine/
[37] "The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites", Parmy Olson. *Forbes Online,* November 20th, 2014. url: http://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/

[38] McReynolds, “China’s Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy.”
[39] Ibid.
[40] “Russia’s Public Stance on Cyberspace Issues”, Keir Giles. *2012 4th International Conference on Cyber Conflict,* CCDOE . url: http://www.conflictstudies.org.uk/files/giles-russia_public_stance.pdf
[41] Keir Giles, “Russia’s Public Stance on Cyberspace Issues,” *4th International Conference on Cyber Conflict*, 2012, 64, http://www.conflictstudies.org.uk/files/giles-russia_public_stance.pdf.
[42] Ibid., 65.
[43] Ibid., 70.
[44] Sebastian Bae, “Cyber Warfare: Chinese and Russian Lessons For US Cyber Doctrine”, Georgetown Security Studies Review, May 7th, 2015. url: http://georgetownsecuritystudiesreview.org/2015/05/07/cyber-warfare-chinese-and-russian-lessons-for-us-cyber-doctrine/
[45] Trepant, Hugo; Jansen Mark; Lamaa Abdulkadaar; “Achieving Information Superiority”, Strategy&, https://www.strategyand.pwc.com/media/file/Strategyand_Achieving-information-superiority.pdf
[46]“Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations”, Roland Heickero. *FOI User Report March 2010,* 25
[47] “Article 51” Charter of the United Nations, http://legal.un.org/repertory/art51.shtml
[48] “White Paper on Defence and National Security.”
[49] The Department of Defense, “The DoD Cyber Strategy.”
[50]*Cyberdeterrence and Cyberwar*, Martin Libicki. RAND Corporation, 2009, 33. url: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
[51] Richard Norton-Taylor, “Britain Plans Cyber Strike Force - with Help from GCHQ,” *The Guardian*, September 30, 2013, sec. UK news, http://www.theguardian.com/uk-news/defence-and-security-blog/2013/sep/30/cyber-gchq-defence.
[52] "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence". Magnus Hjortdal. *Journal of Strategic Security 4*, no. 2 (2011): 1-24. url: http://scholarcommons.usf.edu/jss/vol4/iss2/2
[53] David E. Sanger and Martin Fackler, “N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say,” *The New York Times*, January 18, 2015, sec. Asia Pacific, https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.