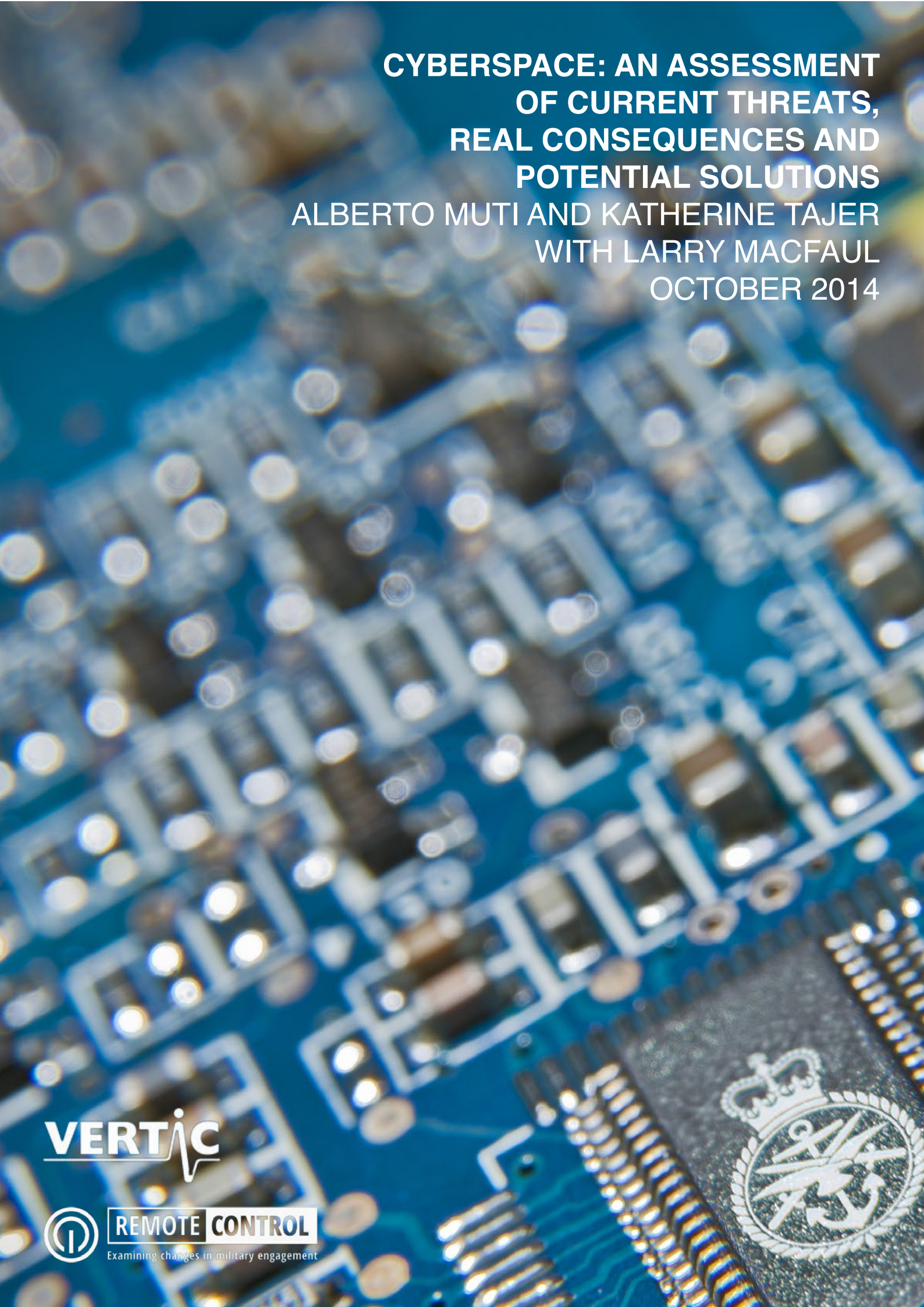

CYBERSPACE: AN ASSESSMENT OF CURRENT THREATS, REAL CONSEQUENCES AND POTENTIAL SOLUTIONS

ALBERTO MUTI AND KATHERINE TAJER
WITH LARRY MACFAUL

OCTOBER 2014

VERTIC

REMOTE CONTROL
Examining changes in military engagement

The Remote Control project is a project of the **Network for Social Change** hosted by **Oxford Research Group**. The project examines changes in military engagement, in particular the use of drones, special forces, private military companies and cyber warfare.

The Verification Research, Training and Information Centre (VERTIC) is an independent, not-for-profit charitable organization. Established in 1986, VERTIC supports the development, implementation and verification of international agreements as well as initiatives in related areas.

Alberto Muti works as a Research Assistant for the Verification and Monitoring programme. He follows a range of international agreements, both existing and proposed, and analyses technical aspects of their implementation and verification. His other research interests include illicit procurement of dual-use items, new technologies, and international security studies, with a focus on Asia. Alberto holds an MA in Non-proliferation and International Security from King's College London and a BA in International Relations from Bologna University.

Katherine Tajer is a Research Assistant at VERTIC and has contributed to the organisation's internal reports on cyber security and arms control. Katherine holds a BA in International Relations from Tufts University. Her previous experience also includes internships with the Institute for Science and International Security and Amnesty International UK.

Larry MacFaul is a Senior Researcher with the Verification and Monitoring Programme where he works on arms control and security, and prior to this, trade and development issues. He has published and spoken widely on these areas. Larry carries out analysis, project development and management, and government capacity-building exercises. His work has covered illicit trafficking in radioactive materials, nuclear safeguards, nuclear disarmament verification, cyber security, conventional arms trade controls, the UN climate change treaty, and illegal trade in natural resources. He works with governments, international organisations, businesses, research institutes and other stakeholders. Larry is editor-in-chief of VERTIC's publication series and a member of the editorial board for the international journal Climate Law. Larry holds a Master's degree from the London School of Economics and a BA Hons from Oxford University.

Published by the Remote Control project, October 2014

Remote Control Project
Oxford Research Group
Development House
56-64 Leonard Street
London EC2A 4LT
United Kingdom

+44 (0)207 549 0298
media@remotecontrolproject.org

http://remotecontrolproject.org

Cover image: The Ministry of Defence badge on a computer chip. The UK is building a dedicated capability to counter cyberspace attacks. © Crown Copyright

This report is made available under a Creative Commons license. All citations must be credited to The Remote Control Project and VERTIC.

Contents

EXECUTIVE SUMMARY

Leaders across the globe have identified cyber attacks as one of the greatest threats facing developed nations. The rising importance of cyber security issues is also part of a global trend of moving towards 'remote control' warfare, that minimizes engagement and risk while extending its reach beyond conflict zones, for example through drone strikes. This paper seeks to examine the role of cyber attacks in remote control warfare, and considers the potential impact of cyber attacks on civilian populations and on future international stability.

The report is divided in four main sections:

1. Cyber attacks in International Relations

This section examines the relevance of cyber attacks to national security. Considering several key examples of cyber attacks, this section will look at markers of national security such as bilateral relationships, and cooperation within international governmental organizations. Additionally, this section will consider international efforts to manage cyber threats, and foster cooperation between states.

2. Cyber attacks as weapons of war

This section will review two examples of cyber attacks in the context of war, and consider the potential of cyber attacks to inflict damage on the scale of a military strike or terrorist attack. While it is possible to inflict material damage and even cause casualties through a cyber attack, an offensive of this kind requires a high degree of expertise and preparation that only national governments have demonstrated to date. Furthermore, cyber attacks offer the opportunity to disable critical infrastructure without using violence, and this option might be more appealing to some actors, especially considering that an attack inflicting damage and human losses would elicit a stronger reaction.

3. Civilian consequences of cyber threats

Section three considers the ways in which cyber threats have extended the arena of total war. Current trends suggest that more people will be subjected to cyber crime and threats, either as the result of inter-state tension or due to the low barrier of entry for criminals for online crime. Given this fact, this section explores how rising internet crime and conflict has and will continue to affect citizens' relationships with their government and military.

4. Main conclusions and moving forward

The final section of this report considers some of the peculiar characteristics of the debate surrounding cyber security and the potential for future instability. It argues that cyber security is a field at high risk of alarmism and threat inflation, and that this dynamic might have destabilising effects in the future. In its conclusion, the report outlines the potential for confidence-building measures and international cooperation at the technical level to counter the destabilising effects of the 'militarisation' of cyber security.

Introduction

In many countries, information technology has become solidly embedded in most facets of human activity, from the operation of large-scale critical infrastructure to individual financial management and leisure.

This report aims to provide a comprehensive overview of the main talking points in the cyber security field and to identify trends that may have an impact on future developments. The rising prominence of cyber security is certainly a product of technological advancement, but it also plays a part in the global tendency to move towards forms of 'security by remote control'. Remote control warfare is pervasive yet largely unseen, maximising the potential to strike at potential threats at any moment while deploying force in an 'efficient' manner that often entails fewer risks for the attacker. The vast reach of the global information infrastructure is simultaneously a weapon, vulnerability and battlefield for remote control war. However, remote control warfare raises many questions with regards to its unintended effects, especially in terms of collateral damage and long-term stability. Considering the key importance of the internet for many civilian activities, such as business, communications, day-to-day bureaucracy and social interactions, it is important to assess what the consequences of militarised cyberspace could be.

This report is divided into four main sections: the first section will examine how the rise of potential threats and vulnerabilities in cyberspace is being addressed in State-to-State relations, and will present some important cases of cyber attacks that have had an impact on foreign policy. The second section will look at the use of cyber attacks during conflicts and at the potential of 'cyber weapons' to cause destruction and casualties on the scale of conventional weaponry. The third section will assess the impact of cyber attacks on everyday life for civilians. Finally, the fourth section will look at current trends in the debate and implementation of cyber security, focusing especially on the potential for future instability caused by present policies, and will outline proposals to mitigate threats.

Vulnerability Versus Threat: The Anatomy of a Cyber Attack

Understanding the anatomy of a cyber attack is an essential prerequisite for understanding the threats created by cyberspace, what actors may be involved, and where and how these threats will play out. A fundamental distinction to make within cyberspace is between vulnerabilities and threats. A vulnerability is the existence of an opening for a cyber threat to take hold – for example – an email account protected by a very simple password, such as '123', may be easier to infiltrate than another. A threat is the combination of this vulnerability with an actor and a motivation. For example, a criminal may want to log into an email account to obtain bank details or national insurance numbers.[1] Throughout this paper, we will aim to maintain a distinction between vulnerabilities and threats, and how they are treated within the world of cyber security.

Different types of vulnerabilities lead to different types of threats. The first and most obvious vulnerability is people: as in the previous example of a weak password, poor IT knowledge or too much trust in a system leads to continual vulnerabilities. The other type of vulnerability is computer based. As computers run on complex and long lines of code, it is likely that an error will exist at some point in the code. Once that mistake is exploited, a vulnerability turns into a threat.

To date, threats, otherwise called attacks or 'hacks' in this paper, have manifested themselves in two main ways: via phishing or malware. Phishing often takes advantage of the human vulnerability, exploiting people's trust and forcing them to give up information. Early forms of a phishing attack are similar to crimes that occurred prior to the internet; like chain letters asking for money, basic phishing attacks include emails offering fake investment schemes or sales offers. More advanced phishing attacks, called spear-phishing, utilise specific knowledge about an individual or network and develop attacks that are more likely to be successful.[2] Alternatively, malware exploits a vulnerability - either human or computer based- and, if successful, leads the infected computer to run a malicious program. Malware can take a variety of forms and produce a variety of ends. A worm, for example, will continue to replicate on all computers on an interconnected system. If the malware turns the infected computer into a 'bot' (also called a 'zombie'), it will carry out automated tasks over the internet without the owner's knowledge, often working as part of a larger network of hijacked computers, called a 'botnet'. Any of these attacks can contribute to a Distributed Denial of Service (DDoS) attack, which floods a targeted website with so many users that it will cease to function. Alternatively, a worm or malware can send messages back about a user's activities, like keystrokes, emails, or even automatically switching on the computer's microphone, to support espionage efforts. Cyber attacks of a larger scale often involve a variety of these threats in tandem - a phishing attack may convince an individual to install malware, which functions as a worm, leading to the creation of a series of botnets.

[1] Pg 38, Singer, P.W; Friedman, Allan. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, Oxford, UK. Copyright 2014.
[2] Singer and Friedman, 41

1. Cyber Attacks in International Relations

This section will discuss how the militarisation of cyber-space has impacted governments globally, and current work taking place to create regulations and norms within the field. To examine how cyber attacks have affected government-to-government relations, we will start by profiling one of the most well-known cyber attacks, Stuxnet, and its consequences. Then, this section will present a variety of international efforts to regulate the arena. Following, we will analyse the cyber attack Estonia suffered in 2007 - looking at who created the threat and how it was responded to. Finally, this section will consider some of the difficulties posed by the attribution of cyber attacks, and how low-level cyber attacks and cyber espionage - both scarcely visible phenomena - can have adverse effects on international relations.

Developed nations like the US and UK have adopted a multi-pronged approach for targeting cyber threats and have integrated cyber security programs across several levels of defence and law-enforcement. The prevention of cybercrime, cyber warfare and cyber-facilitated espionage has become a major objective of a nation's police, military, and government to ensure a minimal cyber disruption within their jurisdiction. The UK's Cyber Security strategy for example, launched in 2011, earmarked £650 million over four years to increase expertise across the Home Office, the Department for Business Innovation and Skills (BIS), the Cabinet Office, the Ministry of Defense, the National Crime Agency, and the Serious Organized Crime Agency (SOCA).[3]

Investing in the Ministry of Defence to combat cyber threats suggests that the UK sees issues of cyber security as issues of national security, but experts still question this association. Historically, any potential threat to State sovereignty, or a State's ability to maintain self-governance and protect its borders, has been classified as an issue of national security. A range of threats varying in severity and longevity may ultimately have an effect on State sovereignty: more conventionally a long-lasting war, and more hypothetically a consistently poor economy, could lead to serious governmental instability. However, the general consensus among cyber security scholars is that the national security implications of cyber threats have been overplayed. As stated by cyber security expert Myriam Dunn Cavelty: 'the threat that they represent to national security has been overstated: despite the persuasiveness of the threat scenarios, cyber-threats have clearly not materialized as a 'real' national security threat'.[4]

To date, the majority of cyber incidents that make the news or affect our daily lives do not impact a State's sovereignty. Considering that the same type of cyber threat that inconveniences an individual for a number of minutes can also cause a government to lose control of its online platforms (DDoS), it is important to define what types of attacks may have a real impact on national security. For this section of the paper, we use a narrow set of criteria to define a cyber threat to national security. An obvious starting point would be a threat to critical infrastructure, as targeting power lines or water sources is a common tactic in modern warfare. Another example of a national security cyber threat would be an attack on government internet infrastructure: websites or interactive online platforms for government initiatives, like a system to pay in taxes or communication between two branches of government, as this may significantly challenge a government's functionality. The final example would be the use of any cyber attack during a physical or 'kinetic' war between two or more States, which is discussed in the next section. As the perception of these potential attacks is viewed as a threat to sovereignty, a State's preventative measures will impact countries' relationships and affect the global state of play.

Stuxnet

An oft-cited example of cyber sabotage entering the realm of national security is the 2010 case of Stuxnet. The attack, referred to as 'Olympic Games' by the US National Security Administration (NSA), is widely thought to have been developed by the American and Israeli governments to set back Iranian progress on the development of a nuclear capability.[5] Stuxnet is an example of both a critical infrastructure attack and a Supervisory Control and Data Acquisition Attack (SCADA): meaning it targeted software that controls an automated activity, such as the signaling network for a railway, or the flow of gasoline through pipes.[6] SCADA presents a growing cyber vulnerability for many States, as more elements of critical infrastructure are maintained through computer systems. Stuxnet targeted Iranian uranium centrifuges that were controlled by a network of in-house computers. In the process of uranium production, a gas centrifuge is designed to spin rapidly to separate the heavier Uranium-238 atoms from the Uranium-235 atoms, which are lighter and used in the production of nuclear weapons. Stuxnet was designed to enter the computer operating system controlling Iran's centrifuges at the Natanz Facility, undetected. As stuxnet was a worm (see section 1), the malware only needed to be installed on one computer to spread to the others on the interconnected system. The code distributed by the worm would cause the centrifuges to spin at such

[3] Pg 25 'The UK Cyber Security Strategy Protecting and promoting the UK in a digital world'. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf November 2011.
[4] Pg 4 Cavelty, Myriam Dunn. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age Center for Security Studies (CSS), ETH Zurich
[5] 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

a high speed that they would eventually break. Current estimates suggest that the worm successfully destroyed around 110 centrifuges.[7]

Iran had a predictable but telling response to the attack. Iran was quick to deny that any infrastructure had been compromised due to cyber infiltration and assured its populace that the Iranian military was prepared to respond to future attacks.[8] A successful cyber attack can undermine trust in a system – whether it targets a bank or a government website.[9] In both corporate and diplomatic spheres therefore, leaders like to appear prepared and invulnerable to future attacks, and may try to keep news of such an attack from being released publicly. In fact, it is argued that a major goal of Stuxnet was to break the confidence of Iranian scientists in their project, and erode trust in the Iranian government.[10] David Sanger, a prominent reporter on the Stuxnet crisis, notes that the virus aimed to make the first few breakdowns appear as accidents. These small but frequent accidents would ultimately cause the scientists to shutdown the plant for several weeks, but still be unable to identify what had gone wrong. The Iranian scientists had already encountered many difficulties while constructing the centrifuges, making this desired outcome all the more likely.[11] Hoping that more elements of the program would not break down, they proceeded with extreme caution, not only continuing to lose centrifuges but also stunting work in other areas of the plant. Ultimately, it was this reaction to the failing centrifuges that actually set back the program more decisively, than the actual damage to the centrifuges produced by the attack.[12]

The ambitions of the Olympic Games operation were eventually its undoing. Several years into the program, in 2010, the US created a more aggressive form of the worm and deployed it onto the Natanz network. The fatal error came however, when a scientist connected his laptop to the system and the worm copied itself onto his computer. When he later plugged the computer into the internet at home, the new form of the worm could not differentiate between the facility and the internet and began to copy itself, moving onto other networks and computers. It was a matter of days before cyber experts like Ralph Langner identified the bug, and, shortly after, the press had unveiled the damage to the Iranian centrifuges.[13] After much suspicion of US involvement in the creation of the attack, in a 2012 article for The New York Times written on the basis of extensive interviews with anonymous Israeli and American officials, David Sanger claimed that the attack was jointly ordered and developed by the United States and Israel.[14]

Questions and Lessons from Stuxnet

Stuxnet was a watershed moment for the use of cyber attacks as a political tool. It is perhaps the first time in US history that an administration turned to cyber-sabotage to promote a foreign policy goal: in this case, the eradication of the Iranian nuclear weapons program. Indeed, since major cyber attacks are not, as far as we know, commonly used by countries to degrade other countries' critical infrastructure, the US may have hoped that Stuxnet could demonstrate that there is a 'smarter, more elegant way' to tackle problems of this nature.[15] Since it is widely believed that Israel was involved in the Stuxnet attack, such a demonstration might have been aimed at persuading the Israeli government that there are better options available to achieve their goals than conventional air strikes.[16]

Secrecy was key in the case of Stuxnet, as it allowed for a prolonged attack that would maximise destruction without the Iranians pushing their nuclear facilities further out of view. Alternatively, a high-publicity attack allows a nation to advertise the extent of their cyber capabilities, deterring other States in the same way that a nuclear weapons test might.

Since a precedent now exists for the use of cyber sabotage from a State against another, it seems plausible to consider that it may be used for a variety of foreign policy and security objectives – either secretly or openly. For example, we could see a cyber attack targeting the same institutions present on a US Treasury sanctions list. Equally, cyber attacks could be used by a government to promote or defend its international standing or reputation, or to bolster soft power strategies. The attack on the New York Times in January 2013, allegedly led by the Chinese government, may have been organised to prevent the publication of an article that could damage the reputation of China's Prime Minister,

[6] 'Supervisory control and data acquisition (SCADA)' Centre for Protection of National Infrastructure, http://www.cpni.gov.uk/advice/cyber/scada/

[7] Albright, David; Brannon, Paul; Walrond, Christina. 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment', ISIS, December 10, 2010. url: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

[8] See source 4

[9] Pg Rid, Thomas. Cyber War Will Not Take Place. Hurst & Company, London, 2013

[10] Ibid.

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

[12] Rid, 32

[13] Sanger, 204

[14] 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%3As%2C%7B%221%22%3A%22RI%3A9%22%7D&_r=0

[15] Sanger, 190

Wen Jiabao.[17] If nations consider that they may legitimately censor content available to their own citizens, it is not surprising that they may wish to censor their critics abroad as well.

Operation 'Olympic Games' also demonstrates the paradox that nations face regarding the weaponization of technology. On the one hand, cyber attacks aligned with political objectives potentially yield strong results with a low financial and resource investment. However, influential governments like the US and UK want to at least publically support the internet as a conflict free, consumer-maintained space that promotes freedom of expression and commercial prosperity, ensures the safety of business activities and individual users. The militarization of cyberspace is ultimately at odds with this goal, especially considering the escalation potential of cyber attacks that will be better discussed below.

Current International Dialogue on Cyber Security - Developing Legislation and Next Steps

States' differing opinions about the role of the internet may be a significant factor behind the lack of international legislation in the field of cyber security. The only existing international attempt has been the Budapest Convention, or Convention on Cybercrime. This treaty targets the important issue of cybercrime but does not tackle any further issues, such as military use of cyberspace. Fundamentally, the convention seeks to unify the understanding of crimes on the internet with those that occur off the internet - some obvious examples including hate speech or the distribution of child pornography. The convention envisages that anything that could be considered cybercrime - which may include distribution of malware - could be mutually enforced across territories, which could help to eliminate the anonymity many criminals gain in cyberspace due to permeable online boundaries between States.

The Budapest Convention is signed by fifty States, but does not have the necessary support within or outside of it to provide seamless enforcement of its objectives, nor does it have any sort of monitoring regime. Another obstacle is Russia and China's non-signatory status. Russia and China's internal efforts to censor their populations is often cited as a reason for their resistance to international efforts. In 2011, China and Russia presented a proposal entitled 'International Code of Conduct for Information Security' (A/66/359) to the UN General Assembly. While the norms and laws suggested in A/66/359 were conventional, the document was received poorly by the Western world as many believed that Russia and China were just reiterating previous ideas from the West in order to appear ready for the first International Cyber security conference, to be held in London that year. In particular, the document's emphasis on State authority over domestic internet-based policy was perceived by the West as a call against cooperative policy.[18]

The UN-level debate on cyber security has harnessed a lot of discussion, but has not necessarily produced concrete results. The first mention of cyberspace took place in the General Assembly in 1998 and the first group of governmental experts (GGE) convened in 2004. It is important to note that this initial meeting of the GGE was unfruitful, and the experts were ultimately unable to produce any resolutions.[19] A new GGE met in 2009/2010, and another at three meetings across 2012 and 2013. The mandate of these groups was to study potential threats in the field and identify areas for cooperation, reporting back to the UN General Assembly on their findings.[20]

Currently, the UN office of Drugs and Crime (UNODC) and the International Telecommunications Union (ITU) are at the forefront of UN initiatives in the cyber arena.[21] The UNODC focuses on cyberspace as it relates to their main areas of authority, more specifically looking at organised crime online and child abuse. The ITU sets international standards in a number of areas, from expanding the accessibility of the internet to working to ensure emergency telecommunication lines.[22] Their work on cyber security is extensive, and includes the development of the Global Cybersecurity Index, which aims to rank States in order of cyber preparedness, as well as the ITU-T 'Study Group 17' which conducts research to ultimately create standards on important vulnerabilities - such as smart phones, cloud computing and social media.[23]
Perhaps the most fully formed attempt to consider the international legal implications of cyber attacks is the Tallinn Manual on the International Law Applicable to

[17] Perlroth, Nicole. 'Hackers in China Attacked The Times for Last 4 Months' The New York Times, January 30th, 2013. url: http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?adxnnl=1&pagewanted=all&adxnnlx=1408032091-pSNo8hrZsqYJv29wmK0chQ
[18] Fansworth, Timothy. 'China and Russia Submit Cyber Proposal'. Arms Control today, November 2011, Arms Control Association online, https://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal
[19] Pg 22. Maurer, Timothy. 'Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cybersecurity', Harvard Kennedy School Belfer Center, September 2011. url: http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf
[20] 'FACT SHEET: DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY', United Nations Office for Disarament Affairs, June 2013. url: http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf
[21] Maurer, 19
[22] 'Key Areas of Actions', International Telecommunications Union,url: http://www.itu.int/en/action/Pages/default.aspx
[23] 'Study Group 17 at a glance', International Telecommunications Union, url: http://www.itu.int/en/ITU-T/about/groups/Pages/sg17.

Cyber Warfare. Developed over a three year period by twenty international legal scholars, the manual sets out ninety five 'rules' covering the legal implications of cyber war on State responsibility, sovereignty, and the role in warfare. These rules attempt to identify in which situations existing international law can apply directly to the cyber realm. However, the manual reveals many instances where the complexities of cyber conflict do not easily adhere to current legislative standards, demonstrating that these inconsistencies may have to be negotiated on a case-by-case basis.

Besides disagreement on the value of the internet, the drafting of laws and international legislation is hampered by the speed of technological advancement. Developing legislation, especially at the international level, is a long process that is often outpaced by these technological changes. For example, the advent of cloud computing and the proliferation of smart phones has altered the landscape of threats and vulnerabilities and has therefore altered considerations for UN resolutions and international conventions. Another oft-mentioned obstacle for international law is the level of shared knowledge and vocabulary required to progress on the subject. Private, public and track two dialogues have dedicated significant time to creating lexicons of cyber security, in the hope that clarity of language will lead to more unified thinking on legislation and the creation of norms.

Estonian or 'Nashi' Attack

The 2007 attack on Estonian government and private sector websites and web-based services is often referred to as a cyberwar and offers an example of a cyber attack that significantly affected international relations. A three-week attack on the Baltic republic warranted a substantial national response, altered the relationship between Estonia and Russia, and caused Estonia to call on NATO for assistance. The attack began shortly after a Soviet statue honoring World War II soldiers was removed from the center of Tallinn several days before an important holiday of Soviet tradition, commemorating the USSR's victory against the Germans in World War II. As a result of the statue's removal, the Russian-speaking population initiated violent demonstrations. Basic, low-tech cyber attacks on governmental websites and the banking system began as the physical riots declined. Over the course of the next two weeks, the cyber attacks increased in sophistication, eventually causing the largest bank in Estonia to cease web operations for over three hours across two days. At its highest point, the attack ran botnets on over 85,000 computers to create the worst DDoS attack to date, eventually bringing down 58 websites at once.[24]

Despite causing a high visibility attack unparalleled in its time, the long-term negative effects of the DDoS were negligible. The attack did, however, lead to further scholarship and efforts to combat cyber conflict - such as the establishment of the NATO-run Cooperative Cyber Defence Centre of Excellence and eventually their publication of the aforementioned Tallinn Manual.

Another important detail of the Estonian attack was the reaction of the international community. The Estonian government argued that a blockade of websites was similar to a blockade of a port and should therefore warrant NATO action.[25] This support never came – so it is fair to assume that as of 2007, NATO did not believe that a cyber attack required their collective action. Since this attack, much reflection has taken place on the validity of Estonia's claim, specifically in the Tallinn Manual. The expert authors of the manual determined in 2013, that the 'the law of armed conflict did not apply to those cyber operations because the situation did not rise to the level of an armed conflict'.[26]

Recent developments suggest that NATO legislation may reflect Estonia's way of thinking during the 2007 crisis. In September 2014, NATO ratified a pledge that would promise joint defense given the instance of a cyber attack on any one of its 28 members. The pledge does not attach any specifics to this pledge however, leading cyber security strategists to believe that execution of this pledge will be complex.[27]

Attribution of the Attack and the Threat of Non-State Actors in Cyberwar

A key feature of this cyber incident was the inability of the target, in this case the Estonian government and companies, to identify the perpetrators. A complex and pervasive botnet attack like this might utilise servers across a number of countries, complicating the process of identifying the origin of the attack. Ambiguity over who the perpetrator was appeared to have two main effects. Firstly, it made it difficult for the Estonian government or its allies to begin to develop an effective response to stop the attacks themselves, even if such a response was technically or politically possible, and secondly, it frustrated efforts to take action against the perpetrators once the attacks ended. Faced with this lack of clarity, national and international actors were compelled to speculate about who the attackers were, based on the evidence they had available and their interpretation of that information. Given the context of the attacks, many in Estonia and beyond believed they were led by the Russian government. At one point, the Estonian government publicly stated that they could trace the attacks back to Russia, but later were unable to produce evidence.[28] Without evidence, it was neither possible to confirm whether the attack was Russian-led,

[24] Rid, 7
[25] Rid 31
[26] Tallinn Manual 75
[27] Lemos, Robert. 'In case of cyber attack: NATO members ready to pledge mutual defense', Ars Technica Online, September 4th, 2014. url: https://docs.google.com/document/d/1MgXO6u9azAQA59k0_LyCUjtOH-8eJ1eI6_WzrC-6YSw/edit#

nor if it involved State actors or non-State actors, or both.

About a year after the event, a pro-Putin Youth group called Nashi (translating in Russian to 'Ours') claimed that they had orchestrated the attacks. The legitimacy of Nashi as an independent youth movement has been heavily questioned, however, as sources suggest that Putin's government funds their activities.[29] Nashi's relationship with the government echoes the ambiguity surrounding the place of non-State actors in many realms of modern warfare.

The possibility of a State sponsored 'non-state actor' has caused difficulty within the field of cyber security and in other theatres of conflict. If a non-state actor is perceived to be a representative of a State, does that raise the status of the event to a potential international conflict? This is a frequently repeated question as terrorism has taken the lead as the most prevalent form of armed conflict. For example, this issue was widely debated after separatist militias in Ukraine shot down a Malaysian Airlines passenger plane on July 17th, 2014, as it was alleged that Russia directly controlled the separatists, which would have made it responsible for the civilian casualties caused by the act. The Tallinn Manual on the International Law applicable to Cyber Warfare has also commented on this phenomenon, stating that financial support alone does not mean that the sponsoring State informed those specific actions.[30] Specifically referring to the Estonian case, the manual confirms that 'there is no definitive evidence that the hacktivists involved in the cyber operations against Estonia in 2007 operated pursuant to instructions from any State, nor did any State endorse and adopt the conduct'.[31]

The Nashi case also illustrates that an attack does not have to be terribly sophisticated to create a response. Cyber attacks have what is often called a low barrier to entry as knowledge about hacking is widely available and free to acquire for anyone with an internet connection. Several prominent examples of terrorist attacks demonstrate the fact that terrorists embrace options with a low-barrier to entry - 9/11 being the most obvious. Hijacking a plane does not involve obtaining or assembling explosives, yet the combined casualties for the date stand at around 2900.[32] Considering the goals of most terrorist and non-State groups, simpler attacks may be the most effective.

The 'Cool' War

Infrastructure-based attacks may receive the most media space, but smaller, repeated infiltrations and attacks also have the capability to impact on a nation and its citizens. A barrage of attacks against banks or financial systems may challenge international trust in a currency or economic system. This alternative style of attack is best illustrated by the term 'Cool War', a term coined by science fiction writer Frederick Pohl in the seventies, and adapted by Foreign Policy CEO and editor, David Rothkopf, to define a current genre of cyber war.[33] The strongest example of Cool War is currently taking place between China and the United States. The suitability of this term is two-pronged: firstly, this type of conflict's reliance on cutting-edge technology is considered 'cool', and secondly, the internet arms race is reminiscent of the Cold War in that it allows for a continual scaling-up of resources and forces. Also similar to the Cold War, it allows for a prolonged war of attrition, with the contestants locked in a constant escalation of small-scale, damaging events taking place regularly over an extended period of time, never breaking out into actual conflict.[34]

Industrial espionage plays an important role in this process, as the internet hosts more company information and financial transactions than ever before. Since espionage does not aim to disrupt or destroy computers and networks, it is likely that it is widespread and unnoticed.[35] Up until recently, no nation had pursued a case against individuals or States that had been involved with economic cyber espionage, due to the difficulty of attribution and the ability to connect the attack to quantifiable damage.[36] In May 2014, however, the United States' Department of Justice charged five Chinese nationals with stealing trade secrets from American defense companies and selling them onto the Chinese government. The five men charged were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA) – a unit which has seen several major cyber attacks traced back to it by security firms like Mandiant. While at the time of publishing, no ruling had been passed, it is fair to say that this case will guide future prosecution of economic cyber-espionage.

[28] Rid, 6

[29] 'Kremlin Kids: We Launched the Estonian Cyber War' Wired Magazine Online, Noah Schachtman. March 11, 2000. url: http://www.wired.com/2009/03/pro-kremlin-gro/

[30] Tallinn Manual, 81

[31] Ibid.

[32] CNN Library, 'September 11th Fast Facts', CNN.com, September 8th, 2014 http://edition.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/

[33] 'The Cold War is history. Now it's the Cool War', Editorial, The Observer, Sunday 24 February 2013. url: http://www.theguardian.com/commentisfree/2013/feb/24/cool-war-cyber-conflict

[34] Rothkopf, David. 'The Cool War', Foreign Policy (online). February 20th, 2013. url:http://www.foreignpolicy.com/articles/2013/02/20/the_cool_war_china_cyberwar

[35] Rid, 82

[36] Ibid.

2. Cyber Attacks as Weapons of War

It is worth noting that to date, military actions often benefit from several supporting elements that are critical or highly significant to the success of the operation. Some of these, for example maintaining secure communication and disrupting or deciphering enemy communications, rely on techniques and technology that are, by now, contiguous to those used for cyber attacks to carry out 'traditional' roles of Signal Intelligence. This section, however, aims to discuss the potential effects and effectiveness of cyber attacks used aggressively during conflicts. When looking at cyber attacks as an instrument of warfare, a primary consideration should be that most cyber attacks of the kind observed today are not instruments of violence per se.[37] Instead, they can be used to disrupt public services, disable and potentially sabotage equipment and infrastructure. Sabotage is, indeed, the only occasion in which a cyber attack can be used for physical violence, aimed at inflicting damage and casualties on a target. It must be noted that even attacks that do not cause extensive damage might have serious consequences, as they could provoke an escalation. The destabilising potential of cyber attacks of all levels of severity will be analysed in section four.

Cyber Attacks in Military Operations

There have been at least two occasions in which cyber attacks were used in conjunction with conventional military operations. On one occasion, a barrage of low-level cyber attacks was used during a ground war. This happened in August 2008 in the context of the Russo-Georgian conflict that arose after the Georgian region of Abkhazia and South Ossetia announced their secession, which was backed by the Russian Federation. Low levels of computer attacks had started roughly a week before the main military confrontation began, but the wave of cyber attacks hit in full force on the same day the main military offensive started in earnest, on August 8th. Like the Estonian attack in 2007, referenced in the previous section, the offensive consisted mostly of the defacement of websites and the disruption of web-based services, striking Georgian banks, private sector entities, and governmental websites. This was likely intended to deny services to the citizens that lived far from the areas directly affected by the conflicts, disrupt the Georgian government's ability to coordinate a reaction and to communicate with the national and international public. As with the Estonian case, the wave of cyber attacks caused some disruption, but had little long-term impact, especially considering that Georgia was less reliant on web-based services than Estonia.[38]

Another example shows the height of efficacy for cyber attacks in a war context. One year before the Russo-Georgian war in September 2007, Israel conducted an air raid against a Syrian facility hidden far from the country's main cities, 140 km from the Iraqi border. The facility, called Al-Kibar, was allegedly a nuclear reactor secretly built with the help of the Democratic People's Republic of Korea for the production of plutonium; a subsequent International Atomic Energy Agency investigation in the ruins of the Al-Kibar site seemed to confirm these claims. To strike the reactor, Israeli forces had to fly over Iraq and most importantly, surpass Syrian air defense positions. In other circumstances, these would have been targeted with anti-radar weapons or engaged via an alternative conventional method. However, it seems that during Operation Orchard (the Israeli codename for the attack), a cyber attack was used to disable the air defence positions silently and allow the Israeli planes to enter Syrian airspace undisturbed.[39]

An attack against a military target of this kind must have been sophisticated, probably exploiting specialized knowledge of the target's technical details to disable it with great precision. Reportedly, the Syrian electric grid and other infrastructures were not affected. It is noteworthy that using a cyber attack instead of conventional means also had the result of avoiding the use of violence.[40] Had Israeli forces engaged the Syrian air defense positions directly, both would have been at risk of being injured or killed. Given the nature of the mission, it seems unlikely that the Israeli decision-makers had the specific objective of avoiding the use of violence; more likely, the approach was chosen because it offered the best chances of penetrating Syrian air defenses undetected and completing the mission. Thus, Operation Orchard stands as an example of a cyber attack making a less violent approach not only viable, but preferable.

Beyond the War Zone: Violence through Cyber Attacks

As noted above with the case of Operation Orchard, cyber attacks may be a desirable option in some situations, as they offer, at least in theory, the chance to disable infrastructure without the need for violent action. The debate on cyber security, however, has often focused on the opposite type of scenario: one in which cyber attacks are unleashed against critical infrastructures in a catastrophic way, resulting in mass casualties and destruction. For example, some have argued that a cyber attack could cause an airplane or a train to crash, or that it could cause the explosion of an oil or gas pipeline, or even a nuclear power plant. A less direct (but not less catastrophic) example is that of a cyber attack striking a hospital, plunging it into chaos

[37] Rid
[38] Rid
[39] Rid
[40] Rid, 34

and potentially cutting its power supply. In scenarios of this kind, cyber attacks could inflict the same damage on the same scale of a conventional attack by an army or a terrorist group, without the need for weapons, personnel and direct, on-site intervention. Moreover, some have speculated that cyber attacks of this kind could be wielded by non-State actors and terrorist groups, which could lead to a 'cyber 9/11' in the future.

These claims have garnered a considerable attention in the media, and have been taken very seriously by decision-makers in many circles. However, no cyber attack has ever demonstrated the ability to inflict physical damage on the scale of a military or terrorist attack, and many cyber security experts have reacted to the prospect of an upcoming 'cyber 9/11', or even a 'cyber Hiroshima' with more pragmatism and less panic.

A SCADA attack as disastrous as those described above requires great expertise, significant resources, and a profound knowledge of the target. This is demonstrated by what we know of the technical aspects of Stuxnet, the only cyber attack so far to physically damage sensitive infrastructures. The team behind 'Operation Olympic Games' knew which industrial control system was used in the Iranian uranium enrichment facilities, and the software that was used to operate it. Furthermore, the team had information about the enrichment centrifuges themselves, and thus knew at what speed to rotate them to inflict the maximum structural damage. Even prior to that, they knew how the facility operated, including how to get their malicious software to infect the right machines. The code developed to attack the facilities was expertly built on this information. Without these foundations, the Stuxnet attack would not have been possible.[41]

This level of technical capacity and preparation is not impossible to achieve, especially in the case of facilities that are not as complex and closely guarded as the Iranian centrifuge plants. However, the requirements represent a significant barrier, and greatly restrict the range of actors potentially able to inflict damage on such a scale. Many experts agree that, at least at the moment, only governments have access to this level of resources, manpower and intelligence.[42]

States might be reluctant to use cyber attacks for such destructive purposes. An attack that caused damage comparable to a military offensive would likely elicit an equally proportionate response, and, as will be discussed more extensively in section 4, in the wake of such an attack the technical barriers to obtaining certain proof of the attack's origin might be overcome by the political will to respond to an act of aggression. Because of this, in such a scenario cyber attacks would lose one of their main advantages, namely the ability to act remotely and face little consequences. Furthermore, a cyber attack able to cause widespread physical destruction would, in almost all cases, be equally able to disable the target without causing physical damage. As demonstrated by Operation Orchard and in keeping with the underlying logic of 'security by remote control', when this option is available, countries might prioritise reaching their objective in a way that is efficient and minimises consequences, rather than inflicting unnecessary collateral damage. The situation may change, for example because of different actors gaining access to sophisticated cyber attack capabilities, and it is likely that a cyber attack will, at some point in the future, cause real damage and casualties.[43] However, at the moment, despite the potentially destructive capabilities of cyber attacks, the flexibility they afford leaves hope that destruction by cyber attack will be the exception, rather than the norm.

3. Civilian Consequences of Cyber Threats

Thus far, this paper has focused on cyber attack damage through the prism of the damage and threats they can cause at a national level and their impact on military decision-making and diplomatic relationships. However, as indicated through the examples listed above, major cyber threat can also have a large effect on the population of a State.

It is important to determine to what extent there is a growing capability and tendency to use remote control warfare in modern conflicts. History provides many examples where remotely controlled actions have been used to help achieve an aim. The difference now may lie in the characteristics of the specific technologies currently used and their impact on the decisions of those using them and those affected by them. Remote control warfare as a method of battle increases the ability to strike a broad range of targets in a way that promises to be both effective and limited in intensity and consequences for the attacker. Drone campaigns are an obvious example of this philosophy, striking targets that are inaccessible to conventional military operations. However, the fact that the vast reach of drone attacks have come at the cost of significant collateral damage, such as an unnecessary civilian death toll, should not be ignored.[44]

As stated throughout this paper, it appears that cyber attacks have not yet been used to cause direct, physical destruction and loss of life on the scale of drone attacks. However, the examples discussed previously show how cyber attacks could continually infiltrate civilian life. If cyber experts could alter the speed of centrifuges to take them out of commission, it is not unrealistic to think that they may have started an internal fire, potentially causing widespread fatality at the facility.

[41] Rid, 44-45. Also see Rid, 72-73
[42] See for example Rid, 168
[43] Rid, 79

Other types of critical infrastructure may provide more obvious targets in a time of war or conflict. Air traffic systems, which are traditionally radar based, are becoming ever more dependent on Automatic Dependent Surveillance - Broadcast, or ADS-B, which utilises GPS to transmit and receive information about planes' positioning and routes. The system has been embraced because it is simple and easy to use, but experts warn that it may also be too easy to exploit. For one, this data is unencrypted – or not specifically coded to prevent unauthorised access. As a result, interference with this data could lead to blocked signals, i.e. planes' locations being hidden from other aircraft. A more technically challenging attack involves the creation of 'ghost planes', where non-existent planes show up on the ADS-B system, causing other flights to change route and potentially crash into one another.[45] This vulnerability has yet to be exploited and is under close examination by aviation authorities across the globe, but does aptly demonstrate the level of reliance civilian activities can have on cyber based systems.

Increased Surveillance as Cyber Security

The impacts of cyber war and other militarised uses of cyber instruments on civilian life are not limited to large-scale sabotage or terrorism. Arguably, the most obvious example of cyber war entering the civilian realm is the extensive surveillance that most of the English-speaking world now faces. The Edward Snowden case and the National Security Administration files that he leaked to the press, exposed the amount of privacy most people forfeit as soon as they log-on. The first article, based on a series of documents leaked to journalist Glenn Greenwald at The Guardian, revealed that 'the communication records of millions of US citizens are being collected indiscriminately and in bulk – regardless of whether they are suspected of any wrongdoing'. These communication records were obtained from the phone company Verizon, revealing that private corporations had few qualms about selling customer data.[46] Documents and articles released over the next few days revealed the full extent of the United State's "PRISM" program, through which the NSA received information from its citizens' search histories, online chats, and emails, from online giants such as Google and Facebook.[47] As the story unfolded, it became clear that the United States had solicited the help of its main allies - the United Kingdom, Australia, and Canada. The UK Global Communications Headquarters or GCHQ played a particularly strong role, providing surveillance information on a number of world leaders during two G20 summit meetings that took place in London in 2009. Allegedly, GCHQ created a variety of traps to pick up participants' emails, Blackberry messages, telephone call logs and occasionally phone calls themselves, by creating fake internet cafes and compromising the guests' IT security.[48]

The revelation of this widespread surveillance network was a considerable shock to most civilians. To date, the impact of the War on Terror had warranted the loss of some civil liberties; however, for many PRISM seemed a step too far. 'The Day We Fight Back' was a widespread and vocal protest that demonstrated general distrust of the NSA and the PRISM system. Taking place on February 11th, 2014 in fifteen countries, the protest highlighted popular and international demand for privacy rights. Within one day, 18,000 calls were placed and 50,000 emails were written to American congressmen and congresswomen demanding action.[49]

The ultimate impact of this protest seems to be minimal, however. The New York Times noted that Wikipedia did not participate, and the level of involvement from many other websites was barely noticeable.[50] It is fair to say, however, that any legislation regarding internet governance or rights has been slow going, and that these protests may still have yet to make their main impact.

4. Main conclusions and moving forward

For many countries, cyberwar is already a reality: cyber security is discussed in the national security strategies of many nations,[51] and States have identified cyber attacks as a relevant and credible threat to their national security. The United Kingdom has listed cyber attacks, conducted by other nations, by terrorist organisations or by organised crime, as the second highest priority threat for the coming years.[52] In addition, countries have started integrating cyber security operations in their military doctrine. In its 2010 Defense

[44] Whitlock, Craig. 'Drone strikes killing more civilians than U.S. admits, human rights groups say', Washington Post, October 22nd, 2013. url: http://www.washingtonpost.com/world/national-security/drone-strikes-killing-more-civilians-than-us-admits-human-rights-groups-say/2013/10/21/a99cbe78-3a81-11e3-b7ba-503fb5822c3e_story.html

[45] Marks, Paul. 'Air traffic system vulnerable to cyber attack', The New Scientist, Magazine issue 2829. url: http://www.newscientist.com/article/mg21128295.600-air-traffic-system-vulnerable-to-cyber-attack.html#.VASb2j777gU

[46] Greenwald, Glenn. 'NSA collecting phone records of millions of Verizon customers daily', The Guardian, 6 June 2013. url: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[47] Greenwald, Glenn; MacAskill, Ewen. 'NSA Prism program taps in to user data of Apple, Google and others', The Guardian, 7 June, 2013. url: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[48] Ewen MacAskill, Nick Davies, Nick Hopkins, Julian Borger and James Ball, 'GCHQ intercepted foreign politicians' communications at G20 summits', The Guardian, 17 June 2013. url: http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits

[49] Gabatt, Adam. 'Protesters rally for 'the day we fight back' against mass surveillance', The Guardian, February 11, 2014. url: http://www.theguardian.com/world/2014/feb/11/day-fight-back-protest-nsa-mass-surveillance

White Paper, the Republic of Korea has mandated the establishment of a 'Defense Information System' to fully include high-technology information capabilities in its military operations, and has founded a 'Cyber Warfare Response Center' to respond to cyber attacks. Almost a decade ago, the US Air Force included cyber security in its mission, adding cyberspace to the realms that USAF 'flies and fights in',[53] along with air and space. Most notably, the United Kingdom has explicitly stated that it is developing not only the capability to defend against cyber attacks, but to 'strike in cyberspace', too.[54]

Given the importance cyber warfare has assumed in the strategic outlook of many nations, it seems fitting that its effectiveness at achieving security and stability is analysed. The previous sections have discussed how cyber attacks are already a relevant part of warfare, and more broadly, an instrument (or, rather, a set of instruments) States use to pursue their security agendas and other interests in the international arena. However, trying to assess the different cases outlined with the same lens may be misleading. On the contrary, it seems important to note that all cyber attacks are not created equal.

Notable instances of cyber attacks have varied in their targets and level of success. At the lower end of the spectrum lies what could be called vandalism: the act of defacing websites and disrupting services, often with little or no long-term impact. Increasing in intensity, we have cases of espionage, some of which directly affected a country's national security interests, while others targeted institutions that were not strictly tied to national security, but were still publicly relevant, such as major media outlets. At the most extreme end of the spectrum, we saw cyber attacks used during military operations, and for destructive sabotage of important national security infrastructures, like operation Olympic Games.

These examples highlight one of the most striking – and often confusing – features of cyber security: its diverse and multidisciplinary nature.[55] Unlike some of the fields it has been compared to, such as nuclear weapons policy, cyber security is not limited to the area of military security. On the contrary, it cuts across most sectors and sections of society and government, from economics and finance to individual and civil rights. The risks associated with cyber attacks go from the mundane, such as the theft of personal data, to the mass-casualty cyber-disaster scenarios outlined in section 2. The diverse nature of cyber threats means that individuals are as likely to suffer because of a cyber attack as governments or large utilities and service providers are. Similarly, potential perpetrators vary wildly, going from vandals and petty criminals to organised crime, terrorist groups and national armies. It is interesting to note that defense against cyber attacks, too, is not handled solely by national governments. States have increasingly sought cooperation with the private sector on initiatives aimed at securing the internet. These go from the protection of critical infrastructure to the involvement of private companies in combating cyber espionage, as in the case of Mandiant. Moreover, some governments have actively sought to raise awareness among their citizens and promote best practices of basic network security, in order to tackle cyber crime.[56]

The Securitization of Cyberspace: Instability through Threat Inflation

The current debate on cyber security has often ignored the diverse range of issues inherent in the field, conflating vastly different problems and repeatedly aiming for hyperbolic statements regarding the potential dangers posed by cyber attacks. This way of looking at cyber security might be one of the greatest sources of instability for the 'cyber realm'. For example, it is interesting to note that what was possibly the least-damaging cyber attack, among the ones taken as example in this work, also provoked one of the strongest reactions in political and military circles, as well as in the media. The 2007 string of cyber attacks against Estonian networks was described by the New York Times as 'the first real war in cyberspace', and the Estonian government called on NATO to intervene in collective self-defense, openly describing the wave of cyber attacks as a Russian aggression, and an incursion into Estonia's sovereignty.[57] This reaction is especially instructive as it resulted from a barrage of attacks that did not cause long-lasting damage to physical infrastructure (or digital systems), nor loss of life, and only disrupted the provision of essential services or trade for a limited period of time.

A useful instrument to understand this process is the concept of securitization. The concept of securitization is used in security theories to describe the creation of a narrative that casts a specific object (often the State) as subject to an existential threat, and thus in need of

[50] Perlroth, Nicole. 'The Day the Internet Didn't Fight Back:, The New York Times, February 11th, 2014 url: http://bits.blogs.nytimes.com/2014/02/11/the-day-the-internet-didnt-fight-back/?module=Search&mabReward=relbias%3Ar%2C%7B%221%22%3A%22RI%3A5%22%7D

[51] The NATO Cooperative Cyber Defence Centre of Excellence maintains a page collecting the official national security strategy and, when present, cyber security strategy documents for both NATO members and nations that are not part of the organisation: https://www.ccdcoe.org/strategies-policies.html

[52] UK National Security Strategy 2010, p.11

[53] Rid, xii

[54] https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit

[55] pp. 1161-1162 Hansen, L. and Nissenbaum, H. (2009), "Digital Disaster, Cyber Security, and the Copenhagen School", International Studies Quarterly, 53: 1155–1175.

[56] http://www.chathamhouse.org/publications/twt/archive/view/198545

urgent protection.[58] A highly securitized debate around cyber security issues could have destabilising effects. Relatively small provocations and low-level incidents could be seen as threats to a nation's security. The difficulties in attributing attacks and the blurred lines between independent individuals and groups, State-sponsored actors and States themselves make it more difficult to create a real casus belli, but on the other hand, they leave the lingering suspect that another State lies hidden behind every incident, damaging trust and hindering international cooperation. Furthermore, the low material risk associated with cyber offensives, especially considering the attribution problem mentioned above, along with the (likely justified) idea that other countries routinely engage in cyber espionage and other forms of cyber attack, provides a strong incentive to take the initiative. In this way, the securitization of cyber security issues fosters the 'Cool War' dynamic of continuous attrition and escalation, and can lead to a 'cyber arms race' between nations.

Furthermore, securitization in this field can directly and profoundly impact civilians' day to day lives, whether or not the countries these individuals belong to are at war or not. Establishing greater government control on online activities can result in greater safety from cyber attacks, as well as threats from terrorism, but this comes with the risk (or, arguably, the inescapable cost) of increasing the degree of surveillance even normal citizens are subject to. The debate around cyber security, however, seems particularly prone to hyperbolic threats and to rampant securitization. One of the key reasons for this is likely the multidisciplinary nature of the debate itself.[59] Discussing cyber security issues requires not only an understanding of political and security dynamics, but also a solid technical understanding of the information infrastructure that surrounds us, and how it can be exploited. While technical and scientific knowledge is relevant in other fields of security as well, for example when discussing nuclear issues, in most cases decision makers in the political and military circles can count on a body of knowledge accumulated and simplified over decades of debate. The technology behind cyberspace, on the other hand, evolves at a rapid pace, and only those that are specialised in the field are generally able to keep abreast of these changes. Because of this rapid pace, it is sometimes difficult to estimate the real likelihood of a postulated cyber attack scenario, and the real potential for damage they entail; similarly, the danger posed by real cyber attacks, when discovered, can be easily overblown, especially in an already securitized environment.

Looking Forward: Maintaining Stability in Cyberspace

One way to counter the rampant securitization of the issue is to ensure that accurate information is available. Especially when a new cyber threat is discovered, disseminating factual information on real risks and possible mitigation strategies can help users to defend themselves more effectively and avoid the panic brought on by sensational reporting. To this end, it seems that Computer Emergency Response Teams (CERTs) might have an important role to play. CERTs are expert groups and emergency response centres that analyse and, in some cases, counter cyber security threats. The first CERT was formed in 1988, in conjunction with the first large-scale network security incident (the 'Morris worm' incident), and these centres have been proliferating ever since. Most CERTs are contracted by universities, corporate entities or government agencies, but recently, their duties have assumed an increasingly public dimension. UK CERT, the UK's first comprehensive, national CERT launched in March 2014, will not only provide responses to emerging cyber threats, but has the explicit mission to raise awareness and facilitate cooperation between stakeholders.[60] While many of the more strictly technical services it provides, such as analysis and sharing of sensitive information on threats and vulnerabilities, are currently focused on large entities that are tied to the nation's critical infrastructure, the UK Government plans to gradually extend the collaboration to other partners in the private sector.

CERTs also have an established history of international cooperation. The Forum of Incident Response and Security Teams (FIRST), an international CERT network founded in 1990, currently connects 305 emergency response teams, across 66 countries.[61] Due to the highly networked and connected nature of 'cyberspace', cooperation between actors is vital for the timely identification of emerging threats. Similarly, collaboration and communication can foster the development and spread of effective defenses, building resilience across the network. International coordination against cyber attacks and other threats is not limited to CERT networks either, as initiatives and Confidence-Building Measures (CBMs) are flourishing. The International Telecommunication Union, the United Nations agency responsible for communication and information technology, has launched the International Multilateral Partnership Against Cyber Threats (IMPACT), a public-private partnership engaged in emergency response and capacity building for its member States. IMPACT operates the Global Response Centre, a threat and emergency response center that leverages IMPACT's wide cooperation network.

[57] Hansen, Nissenbaum, 1169.
[58] Barry Buzan, Ole Wæver, and Jaap de Wilde, Security: A New Framework for Analysis (Boulder: Lynne Rienner Publishers, 1998), p. 25
[59] Hansen, Nissenbaum, pp. 1167-1168
[60] https://www.gov.uk/government/news/uk-launches-first-national-cert
[61] http://www.first.org/members/map

Interestingly, the GRC was created using the structure of the Center for Disease Control and Prevention, a high-level public health institution located in Atlanta, USA, and specialised in controlling and preventing disease outbreaks. In addition, IMPACT offers online platforms that allow field experts to share information securely and to provide early warning to the relevant authorities.[62]

Cooperation at the expert level, such as between CERTs and other track two initiatives, seem particularly promising for the field of cyber security, as international legislation and other forms of official intergovernmental action on the matter have progressed slowly. By helping the spread of best practices at a dynamic pace, which keeps up with technological developments, cooperation between CERTs and similar bodies can lay the groundwork for nascent norms and more elaborate international arrangements in the future.

Communication & Information Exchange for the Attribution of Cyber Attacks

Increased cooperation and information sharing at the technical level could also indirectly help solve one of the most challenging issues in the cyber security realm, namely the problem of attribution. Correctly identifying the author of a cyber attack is extremely complex, and in many cases may not be possible at all. Much has been said, especially in military circles, about developing a system that will promptly locate the perpetrators of an attack, but it seems unlikely that a technical solution will appear anytime soon.[63] One of the main challenges is that forensic data, especially data regarding the digital 'path' the attack has followed to reach its target, may not be available to the victim without the collaboration of other States. This is because the physical infrastructure that sustains the internet is spread globally; because of this an attack might pass through servers and connections that are under the jurisdiction of several nations.

Indeed, it has been argued that the main problem regarding the attribution of cyber attacks is political, rather than technical, and that a political solution exists. According to this argument, the difficulty of attributing an attack is a function of the attack's severity. An extremely serious attack – for example, disruption of a national power grid - would elicit a strong political response that could lower the standards of proof 'not to the unreasonable, but to the realistic'.[64] Furthermore, a severe attack could result in higher levels of cooperation from other States in the investigation, providing forensic data obtained from infrastructure under their jurisdiction. In some cases, especially when the affected State is powerful or influential in the international arena, refusing to cooperate with an investigation could be seen as very suspicious, if not as an implicit admission of guilt.[65]

The previous argument is built on a very specific case: an extremely serious attack, causing a strong political response. So far, no known cyber attack has had this kind of impact, with the potential exception of Stuxnet, in which case Iran's international isolation prevented it from exercising this kind of pressure. However, this way of looking at the problem of attribution highlights that communication and information exchange is important not only on a technical level, but also on a political one. Over time, these measures could prove fruitful beyond the worst-case scenario of a highly damaging attack, and could help foster a safer cyber security environment. If States manage to establish a sustained practice of cooperating against cyber attacks and routinely sharing information, the decision by a State not to release forensic data after an attack might prove as telling as the data itself, and provide the international

[62] https://www.gov.uk/government/news/uk-launches-first-national-cert
[63] Rid, 141
[64] Rid, 161
[65] Rid, 162

Remote Control Project
Oxford Research Group
Development House
56-64 Leonard Street
London EC2A 4LT
United Kingdom

+44 (0)207 549 0298
media@remotecontrolproject.org

www.remotecontrolproject.org