Conceptualising Cyber-Security: Warfare and Deterrence in Cyberspace

Muhammad Shoaib

Introduction

In the contemporary strategic discourse, cyberspace is fast gaining importance as a domain of war in addition to land, sea, air and space. States have started to incorporate strategies and tactics to attain reliable levels of security in this domain. Also, in recent years, certain events have brought significant attention toward cyber related matters. Certain major cyber-attacks have become a matter of concern for states due to the threat they pose to national security. Moreover, Cyber-attacks have become important because they are a potential foreign policy and military tool that can be added to existing options in the arsenals of states.[1] Although, for the time being, no cyber-attack is known to have caused death or physical damage to human beings, an ever-growing number of states around the world are preparing for conflict in the cyber domain, and, in this context, have been developing national doctrines, cyber-defence strategies and defensive and offensive capabilities for cyber-warfare.[2] The cyber domain has gained prominence as a subject of political, diplomatic, economic and military debate, at both national and international levels.

Although terms including cyber-security, cyber-attack, cybercrime, cyber-war and cyberterrorism have entered the public discourse; there is no consensus yet on their definitions, making it difficult to create a conceptual framework in which relations and international agreements related to cyberspace can be developed. Military forces around the world also remain concerned about the increasing vulnerabilities related to cyberspace and the

internet. In this context, claims that cyberspace is the fifth domain of warfare have led to a growing debate about the advent of cyber-warfare.[3] Although scholars and analysts have conducted significant research on issues related to the cyber domain, a gap still exists in common knowledge about these terms. It is therefore essential to have a clear concept of cyberspace and cyber-security. This study attempts to provide an understanding of the cyberspace and why it is being incorporated into the realm of security studies.

The 2007 cyber-attack against the Estonian government is an example of conflict in cyberspace. The Distributed Denial of Service (DDoS)[4] attacks against the Estonian government led to an immobilisation of public services in the country for three weeks. The attacks also marked the beginning of joint efforts to address the cyber-warfare threat and to develop international norms for conduct in cyberspace. Similarly, during the 2008 Russian–Georgian war, media and government websites in Georgia came under attack from hackers.[5] In 2010, the 'Stuxnet' computer worm, considered one of the most sophisticated cyber weapon and a possible first incident of cyber-warfare, damaged uranium enrichment centrifuges at Iran's Natanz nuclear site. Stuxnet was compared to a 'cyber missile', aimed at destroying the physical infrastructure of Iran's nuclear plants.[6] According to a report by the *New York Times*, it was a joint US-Israel project, which destroyed roughly a fifth of Iran's nuclear centrifuges.[7] It was a covert operation, known as Olympic Games, and was secretly ordered by president Obama soon after resuming office. The programme was a continuation of the attacks started by president Bush. In 2012, a DDoS campaign against the US financial sector (Operation Ababil) was claimed by the group 'Izz ad-Din Al Qassam', in retaliation for the Stuxnet attack.[8]

Another example of an international conflict created by issues involving cyber-security could be Edward Snowden's 2013 leaks, where he revealed classified documents about the US government's surveillance programmes. The initial leaks were reported by the *Guardian* in June 2013, based on top-secret documents that Snowden stole from the US National Security Agency (NSA). The Snowden leaks revealed how the NSA, through its massive surveillance programme, collected online data of its own citizens and also hacked into the communication systems of foreign countries including allies.[9] The NSA accessed and collected data through back doors into US internet companies such as Google and Facebook with a programme called Prism.[10] Snowden also revealed that the NSA was hacking computers in Hong Kong and mainland China, including their military systems.[11] Further leaks revealed that Britain's intelligence agency GCHQ also aided NSA's surveillance programme by intercepting phone and internet communications of foreign politicians attending two G-20 meetings in London during 2009.[12] The GCHQ also taps fibre-optic cables to collect and store global email messages, facebook posts, internet histories, and calls, and then shares the data with the NSA.[13] Following these leaks, Snowden was given asylum in Russia. While the US considers Snowden a criminal and threat to its national security, Russia refuses to extradite him and calls him a human rights activist.

Even as the Obama Administration accused Snowden of espionage, both China and Russia praised his role and decision in revealing the details of the NSA's secret surveillance programme.[14] Following the revelations that the NSA also spies on its own allies, former Brazilian president, Dilma Rousseff, indefinitely postponed her October 2013 state visit to the US.[15] She expressed anger and frustration that the NSA had intercepted her private

communications, hacked into the state-owned Petrobras oil company's network and spied on Brazilians who had their personal data stored on the networks of US' social media companies.

China also expressed anger towards the US following the Snowden leaks. In a main heading on the front page of the overseas edition of the People's Daily, the Chinese government said the alleged attacks by the US on many networks in Hong Kong and China, including those of Tsinghua University, and Chinese mobile companies were matters of grave concern.[16] The piece also noted that the Chinese government had taken the issue to the US government.[17] The Snowden case is an indication that China-US and Russia-US relationships deteriorated due to cyber-security.[18] Russia granted Snowden asylum despite fierce protest from the US government. So far, these governments have failed to engage in substantive cooperation on issues that are important for global cyber-security.[19]

Following the 2016 US presidential elections, US and European intelligence officials raised alarms that Russia had allegedly influenced the US elections through cyber-attacks and information warfare. According to CIA officials, hackers backed by the Russian government broke into email servers at the Democratic National Committee (DNC), and stole emails from senior members of Hillary Clinton's campaign, including campaign chief John Podesta and Clinton herself.[20] The circumstantial evidence here is that material from the thefts was passed along to WikiLeaks, which then posted a selection of what it received. The Russians also hacked the Republican National Committee and deployed a campaign of information warfare, involving fake news and tweets.[21] Moreover, during the 2017 French presidential elections, it was suspected that Russia

carried out cyber-attacks to influence the presidential elections in favour of Marine Le Pen, and against Emmanuel Macron, by hacking e-mail servers and campaign website of the latter.[22] France also warned Russia against meddling in the elections. Furthermore, the intelligence chiefs of three European countries – Germany, Sweden and the UK also raised similar concerns about Russian attempts at electoral influence.[23] Russian President, Vladimir Putin, however, dismissed accusations of aiding US elections as unproven "rumours" used for internal politics.[24] President Putin said, "We never interfere in other countries' politics and we want no one to meddle in ours." Moreover, during a press conference, President Putin again rejected accusations of meddling in politics of foreign countries. He insisted the Russian state has never been involved in hacking and could not influence foreign elections.[25]

The above discussion signifies that the cyberspace has brought in new dimensions and complexity to national security and international relations. However, unclear and limited understanding of the cyber domain may pose difficulties in devising a credible cyber-security policy. For this reason, it is imperative to understand different concepts in the cyber domain. This study focuses on the following questions: What is cyberspace? Is it a fifth domain of war after land, sea, air and space? What is cyber-security and cyber-warfare? Is viable deterrence achievable in the cyber domain? The study is descriptive and explanatory in nature. In order to comprehend the relation between security and cyber affairs, understanding the cyberspace is a requisite.

Understanding Cyberspace

In simple terms, cyberspace can be defined as a global medium for communication and information exchange

between computers and their human operators.[26] It provides an environment in which sending, receiving and processing of digital signals is possible. This environment is commonly known as the internet. Concurrently, cyberspace is more than just the internet, because every transaction or event which is not happening in the real world is occurring in cyberspace. An example would be the calculation in a single chip or the communication between certain chips which are not connected to the internet.[27] The data or information being processed inside a computer, and not visible to the real world, is also a part of the cyberspace. Similarly, the sharing of data or information through non-internet methods, such as local networks, Wi-Fi and Bluetooth, are also part of cyberspace.

Joseph Nye, an American political scientist, defined Cyberspace as the "Internet of networked computers but also intranets, cellular technologies, fibre optic cables, and space based communications." [28] Cyberspace refers to not only all of the computer networks in the world but also to everything they connect and control.[29] According to the US Department of Defence,[30] "Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". From these definitions, it can be assumed that cyberspace is a variety of networked systems created by connecting electronic components using signals (electromagnetic energy) and software. More importantly, cyberspace was created so that people could create, store, modify, and transfer data and information more easily and rapidly.[31]

Unlike the other domains of land, sea, air and space, the cyberspace is not a physical place; it cannot be measured

in any physical dimension. Apart from the internet, cyberspace includes transactional networks that do things like sending data about money flows, stock market trades, and credit card transactions.[32] In addition, there are some networks which are Supervisory Control and Data Acquisition (SCADA)33 systems that just allow machines to speak to other machines: control panels communicating with elevators, generators, etc.[34] These are systems of combined software and hardware elements that allow industrial organisations or users to control industrial processes. For example, controlling a machine in an industry through a software on a computer. Thus, cyberspace comprises billions of computers, servers, routers, switches, fibre-optic cables, and wireless communications that allow critical infrastructures to work. These networked and interconnected information systems reside simultaneously in both the physical and virtual spaces, and within and outside of geographical boundaries. Their users include nation-states and their component organisational elements and communities as well as individuals and trans-national groups who may not be a part of any traditional organisation or national entity. This explanation of the cyberspace implies that it can signify commercial, economic, cultural, political and social opportunities. Not only that, the cyberspace remains a challenge also because it could become a source of insecurity, instability, crime and competition.[35] Malicious actors may use cyberspace for their selfish motives. Such activities in cyberspace could be detrimental to relations between states and could be a source of distrust and conflict between them.

While international law has still not been defined over the conduct in cyberspace, some analysts argue that cyberspace is the newest and most important addition to the global commons, which comprises four domains: maritime, air, space, and now cyber.[36] Global commons

are environments that are beyond the jurisdiction of any state and are open to everyone[37]. Outer space, maritime and air are the international oceans and skies that do not fall under the jurisdiction of any nation. Just like the other global commons, cyberspace is the domain in which continued unrestrained access can never be taken for granted as a natural and assured right. Outer space begins at a point above the earth where objects remain in orbit. Cyberspace is the electromagnetic spectrum (EMS) that enables digital processing and communications.[38] The maritime domain has been used by humans for thousands of years, air for a century, and space for six decades. Cyberspace is the newest yet most important of the global commons and has been available for less than thirty years, yet more than a quarter of the world's population now uses it every day, and the number continues to expand.[39] Thus, cyberspace has become the centre of gravity for the globalised world and for nations. Cyberspace is crucial not only for military operations but for all aspects of national activity including economic, financial, diplomatic, and other transactions.

Although, cyberspace is qualitatively different from the sea, air, and space domains, yet it both overlaps and continuously operates within all of them. It is the only domain in which all instruments of national power – diplomatic, informational, military, and economic – can be concurrently exercised through the control of data and gateways.[40] Cyber-security has become a vital component of the global security paradigm, as it is a medium which in today's world connects every critical infrastructure including governance, communication, economic and transport. It is being considered as a new medium of warfare, where states and non-state entities could adopt strategies and methods to inflict a cyber-war. The cyberspace is unique because it is intangible and is able to reach and affect other critical infrastructures.

The Concept and Elements of Cyber-security

As discussed in the previous section, cyberspace can be categorised as an operational space, where actions take place by using technology to create an outcome or achieve an objective. These outcomes can be pursued solely in cyberspace or in and across the other operational domains and elements of power. In this sense, it is like any of the other four physical domains – land, sea, air, and outer space – in which humans operate. By this explanation, cyberspace could be viewed within the bounds of the operational domains and elements of power within which the national security community operates.[41]

With the development of the internet as a global infrastructure for business and as a new tool for politics, espionage and military activities, cyber-security has become the central topic for both national and international security. Several characteristics help to establish the perception of cyberspace as an inherently insecure environment. Although cyberspace functions like other domains, there exists uncertainty in the evaluation of offensive and defensive capabilities of oneself and of the adversary. Cyber-weapons are essentially computer codes used to inflict harm,[42] meaning that unlike the physical domain, the virtual nature of malware makes it very difficult for states to gain an accurate picture of the other's capabilities. Cyber-security involves protecting information and systems from major cyber threats, including cyberterrorism, cyber-warfare, and cyber-espionage.

Moreover, cyber-security, to counter cyber-attacks carried out by various actors e.g. criminals, hackers or governments, has become an important policy issue in many states. [43] In order to develop a better understanding

of the concept of cyber-security, the concept of cyber-power must be taken into account.

Cyber-power

The concept of cyber-power is a relatively new one. It is the sum of strategic effects generated by cyber operations in and from cyberspace. Daniel Kuehl, a professor at the School of Information, Warfare and Strategy, National Defence University, USA has given a definition of cyber-power. According to him, "cyber-power is the ability to use cyberspace to gain advantages and influence events in other operational environments and across the instruments of power."[44] The strategic purpose of cyber-power is to attain the ability to manipulate perceptions of the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment.[45] Cyber-power depends on the resources that characterise the domain of the cyberspace. It is the capability to control Information Technology (IT) systems and networks in and through cyberspace. According to Franklin Kramer, national security and international affairs expert from the Atlantic Council, "Cyber-power is the use, threatened use, or effect by the knowledge of its potential use, of disruptive cyber-attack capabilities by a state."[46] According to Joseph Nye, cyber-power can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace.[47] Accordingly, cyber-power is the sum of both soft and hard power in the cyber domain. It can be used to target perceptions and perspectives and at the same time it can also inflict considerable physical damage to critical information systems and even limit the performance of hardware devices. Hence, the element of information is closely related to cyber-power.

Cyber-power also greatly impacts political and diplomatic affairs. The world's most prominent influence medium remains satellite television, which is carried by systems and networks that connect via cyberspace. Militarily, cyber-power has been perhaps the most influential instrument of the last two decades.[48] Cyberspace and cyber-power remain a crucial element of new concepts and doctrines. Across the levels of conflict, from insurgency to main-force conventional warfare, cyber-power has become an indispensable element of modern technologically based military capability.[49] Hence, cyber-power carries the ability to integrate and generate a combined effect of all the other elements and instruments of power and connects them in ways that enhance all of them.[50] This means that cyber-power is the latest technological power that connects and controls all other elements and domains of power including conventional and nuclear, thereby making it a necessity in the modern world. The integration of cyber and other elements of power has also made states more vulnerable as cyberspace can now be used to control or inflict damage to their ability to utilise power effectively. Employing and exploiting cyber-power to be used in cyber-wars has become important for states. Contemporary security studies have now started to focus on cyber-power and cyber warfare as an important issue area.

Defining Cyber-warfare

As with the term cyberspace, there is no universally accepted definition of cyber-warfare. The definitions of explanations about cyber-warfare and cyber-defence are still widely debated, and have become an important topic for international legal scholars, along with governments and international organisations. Contrasting views shape the debate regarding the legality and usage of the term "cyber-warfare". Experts also remain divided over the

reality of cyber-warfare. While recognising the risks connected to the new cyber threats and the necessity of cyber-security, cyber-warfare, according to some experts, is an inappropriate analogy.[51] For others, although cyber war will not replace conventional kinetic (traditional war) operations, armies will increasingly make use of cyber operations to support deployments.[52] This signifies the importance of the cyber domain as it could be exploited to support war fighting in physical domains. Since cyberspace itself could be a medium of war or it could bolster the war fighting capabilities in other domains of warfare, it may be a foregone conclusion that cyberspace cannot be separated from kinetic warfare.

Currently there are differing views over what constitutes an act of cyber-war and what the appropriate response might be, a definition of what constitutes cyber-warfare and whether it encompasses more than states as actors. For example, the US Department of Defence has defined cyber warfare as, "an armed conflict conducted in whole or in part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber-attack, cyber-defence and cyber enabling actions."[53] According to one general definition, "cyber-warfare refers to a massively coordinated digital assault on a government by another, or by large groups of citizens. It is the action by a nation-state to penetrate another nation's computers and networks for the purpose of causing damage or disruption."[54] However, it adds that "the term cyber-warfare may also be used to describe attacks between corporations, from terrorist organisations, or simply attacks by individuals or hacktivists."[55] Following are a few definitions encompassing cyber-attack, network attack and cyber operations;

According to Shane Coughlan, an expert in communication methods and business development, "Cyber-warfare is symmetric or asymmetric offensive and defensive digital network activity by states or state-like actors, encompassing danger to critical national infrastructure and military systems. It requires a high degree of interdependence between digital networks and infrastructure on the part of the defender, and technological advances on the part of the attacker. It can be understood as a future threat rather than a present one, and fits neatly into the paradigm of Information Warfare."[56] According to another definition by the US Department of Defence, cyber operations are "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[57] A computer network attack is defined as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and network themselves."[58] Similarly, a 2001 Congressional Research Service Report notes that "cyber-warfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same."[59] A later report defined computer network attacks as "operations to disrupt or destroy information resident in computers and computer networks."[60] A further definition of cyber-war is "a conflict that uses hostile, illegal transactions or attacks on computers and networks in an effort to disrupt communications and other pieces of infrastructure as a mechanism to inflict economic harm or upset defences."[61] And finally, according to a recent UN Security Council Resolution, "Cyber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state, or private property within another

state including: intentional access, interception of data or damage to digital and digitally controlled infrastructure. And production and distribution of devices which can be used to subvert domestic activity."[62]

Cyber-war may be initiated by state as well as non-state actors against any other state or party with the aim of inflicting damage or gaining control over its cyberspace activities. A successful cyber-war depends upon two things: means and vulnerability. The means are the people, tools, and cyber weapons available to the attacker.[63] The vulnerability is the extent to which the enemy's economy and military use the Internet and networks in general.[64] Exact cyber-war capabilities of states remain largely unknown. However, a growing number of states have organised cyber-war units and ever more skilled Internet experts for combat in this domain.[65] Hence, cyber-warfare can be regarded as a real domain which can influence other domains of warfare. The outcome of waging a cyber-war greatly depends upon the type of attack or offence. The combat and defence strategy in a cyber-war also depends upon the nature of threat or actual offence.

Cyber-attack (offence)

Cyber-war exists in the military and intelligence realm and refers to conducting military operations based on information-related principles. It means disrupting or destroying information and communication systems using cyber-weapons. It also means trying to know everything about an adversary while keeping the adversary from knowing much about oneself.[66] Cyber-war is a conflict in virtual space with means of information and communication technology (ICT)[67] and networks. Like other forms of warfare, cyber-war aims at influencing the will and decision making capability of the enemy's

political leadership and armed forces in the theatre of Computer Network Operations (CNO).[68] CNO is important because it provides both offensive and defensive capabilities in a cyber war.

Three forms of Computer Network Operations can be distinguished:[69] (1) Computer Network Attack – operations designed to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers or networks themselves; (2) Computer Network Exploitation, which means retrieving intelligence-grade data and information from enemy computers by ICT means; and (3) Computer Network Defence, which consists of all measures necessary to protect own ICT means and infrastructures against hostile Computer Network Attack and Computer Network Exploitation. Thus conceptually, Computer Network Operations cover only a narrower section of all cyber-attacks. However, the potential for damage that cyber-war can inflict on national and economic security of a state could be large.

Computer Network Attack, or the deliberate paralysation or destruction of enemy network capabilities, is only one of the many instruments in the domain of military missions. While the importance of Computer Network Attack will certainly increase in the coming years, with regard to the state of developments in offensive cyber-war capabilities, there is still a lack of established knowledge about Computer Network Attack capabilities already available. According to analysts, there are also expectations that the future will bring not only an arms race in cyberspace, but also strategic cyber-wars.[70] Conducting an information operation of strategic significance would not be easy, although not impossible.

Another important aspect is that uncontrollable adverse effects in the highly networked virtual space constitute considerable risks for an attacking state. This factor is relevant because the states that are most likely to develop the technological know-how for strategic cyber-war also become vulnerable due to their increased involvement in cyberspace. Due to uncontrollable side-effects, a cyber-war would also undermine trust in cyberspace over the long term, with possible adverse effects for the global economy, and for all parties involved.[71] The fact remains that no one really knows how destructive a strategic cyber-attack in a conflict conducted in the virtual realm would be.

If a strategic cyber-attack is less likely to be decisive, then cyber-warfare capabilities at the operational level, for actions against military targets during a real war, might become more important. Operational cyber-war capabilities may be developed because a damaging cyber-attack may facilitate military operations, and the capability seems relatively inexpensive. However, for operational cyber-war to work, its targets have to be accessible and offer vulnerabilities.[72] These vulnerabilities have to be exploited in ways the attacker finds useful.

Prediction of the effects of operational cyber-attacks is undermined due to the complexity in carrying out these attacks. Investigations may reveal that a particular system has a particular vulnerability. However, predicting what an attack can do requires knowing how the system and its operators will respond to signs of dysfunction, and knowing the behaviour of processes and systems associated with the system being attacked.[73] Such operations are more likely to confuse and frustrate operators of military systems temporarily because, due to the increasing innovation, even the best cyber-attacks

have a limited shelf life. Thus, cyber-war at the operational level may be a support function for other elements of warfare in facilitating a combat operation.[74]

Following the existence of threat of cyber-attacks, cyber defence remains a concern for the armed forces in cyberspace. Although, majority of attacks in the cyberspace are against internet-connected computers, more advanced attacks may find their way into the network systems through other communication channels also. Many civilian systems can also become victims of cyber-attacks, therefore, a purely military approach to cyber-security defence is not sufficient. The armed forces have an important role in protecting their own systems and in developing potential offensive capabilities. In order to create defences for military networks, the knowledge of defence requirements for civilian networks is required. Although the basics are same for both, military networks differ from civilian ones in important ways. Hence, the armed forces must think hard as they craft their cyber defence goals, architectures, policies, strategies, and operations.

Aggressive actions against an IT system or network can take two forms: cyber-attack and cyber exploitation.[75] A cyber-attack is the use of deliberate actions to alter, disrupt, deceive, degrade, or destroy adversary IT systems and networks or the information and programmes resident in or transiting these systems.[76] Cyber exploitation is the use of operations to secretly obtain information, and is conducted with the smallest possible intervention that still allows extraction of the target information.[77] These should not disturb the normal functioning of the systems. The best cyber exploitation is one that a user never notices.

Cyber-attacks and cyber exploitations are possible only because IT systems and networks are vulnerable. Most existing vulnerabilities are introduced accidentally through design or implementation flaws.[78] As long as nations rely on IT systems and networks as a foundation for military and economic power, and as long as these are accessible from the outside, they remain vulnerable to attacks.[79] Cyber-attacks and cyber exploitation require vulnerability, access to that vulnerability, and a payload to be executed. The primary technical difference between cyber-attack and cyber exploitation is in the nature of the payload to be executed. A cyber-attack payload is destructive whereas a cyber exploitation payload acquires information or intelligence non-destructively. Therefore, the nature of offence in cyber domain depends upon the type and nature of weapon as well as the payload it carries to be used in the cyber-attack.

Cyber-weapons

Payload is the term used to describe things that can be done once vulnerability has been exploited. For example, if a software agent, such as a virus, has entered a given IT system, it can be programmed to do many things – reproduce and retransmit it, and destroy or alter files on the system. Payloads can have multiple programmable capabilities. Moreover, the timing of actions can also be varied, and if a communications channel to the adversary is available, payloads may be remotely updated. In some cases, the initially delivered payload consists of nothing more than a mechanism for scanning the system to determine its technical characteristics, and another mechanism through which the adversary can deliver the best software updates to further the compromise.[80]

Some proponents think that cyber-war will sooner or later replace kinetic war. More frequently, cyber-war is

presented as a new kind of war that is cheaper, cleaner, with less or no bloodshed, and less risky for an attacker than other forms of armed conflict. This seems to make cyber-war more attractive. A cyber-attack like any conventional or a nuclear attack involves weapons. In the cyber domain, these weapons are known as cyber-weapons and there are various types. The working mechanism of cyber-weapons can be compared to kinetic war weapons.

In the context of kinetic war and weapons used, a missile comprises three basic elements: (1) a delivery vehicle i.e. the rocket engine, (2) a navigations system which tells it how to get to the target, and (3) the payload – the components that cause harm. The same three elements appear in the design of a cyber-weapon. There are numerous methods of delivering cyber weapons to their targets. Emails with malicious code embedded or attached is one mechanism of delivery. Another is websites that have malicious links and downloads. It can also be done by wireless code insertion transmitted over radio or radar frequencies.[81] Hacking is a manual delivery vehicle that allows placing the malicious payload on a target computer, system or network. Counterfeit hardware, software, and electronic components can also be used as delivery vehicles. Just as the navigation system guides a missile, it allows the malicious payload to reach a specific point inside a computer, system or network. System vulnerabilities are the primary navigation systems used in cyber weapons. Vulnerabilities in software and computer system configurations provide entry points for the payload. These security exposures in operating systems or other software or applications allow for exploitation and compromise. This enables unauthorised remote access and control over the system.[82]

Whereas, the payload of a missile is the warhead which is packed with some type of 'explosive,' the payload of a cyber weapon is usually a programme that copies information off the computer and sends it to an external source. It could also be a programme that is altering and manipulating information stored on the system. Finally, it could enable remote access so that the computer may be controlled or directed over the Internet. A 'bot'– a component of a botnet[83] – is a good example of a payload that makes possible the remote use of an IT system by an unauthorised individual or organisation.[84] The three-element architecture demonstrates how advanced and sophisticated cyber weapons have become. The architecture creates reusability and reconfiguration of all three components. As software or system vulnerability is discovered, reported, and patched, that component can be removed and replaced while the other two components still remain viable. Not only does this create flexibility, it also significantly increases the productivity of cyber-weapons.

Unlike nuclear or other weapons of mass destruction, cyber weapons and cyber-attacks require less infrastructure, and no restricted materials or knowledge which is in short supply. Cyber weapons have become easier to obtain and use, much more powerful, and ever more sophisticated. Botnets, for instance, which are used for launching Distributed Denial of Service Attacks (DDoS), comprise advanced remote exploitation capabilities within as many computers as a hacker can compromise all over the world. These well disguised programmes have several advanced capabilities. The characteristics of the 'Storm' worm, for example, a Trojan horse spread through email, includes self-transforming i.e. It changes code to evade anti-virus; self-defending i.e. if you try to delete it copies itself; self-replicating i.e. it identifies and infects other

computers; self-encrypting i.e. it can encrypt and decrypt itself to elude signature detection; and self-masking i.e. it changes its communications path to obstruct tracking.[85]

Examples of Cyber-attack (Cyber-offence)

There have been several cases of successful cyber-attacks destroyed entire information systems. The vast 'Storm' botnet detected in 2007, running on 20 to 115 million computers, increased its capacity constantly as more and more computers were compromised. In 2010, there was an increase in the scale, frequency, and severity of DDoS attack activity on the Internet. For the first time an attack of 100 Gigabytes per second (Gbps) bandwidth was reported.[86] That represents a sharp increase in the amount of information that is piled up on a network in order to shut it down. In 2005, the Dutch police found a 1.5 million-node botnet.[87] Estimates suggest that the botnet could generate more instructions per second than many of the world's top supercomputers. With so much power, attacks with devastating consequences can be launched.

The 2009-2010 cyber-attacks against Iranian nuclear facilities are also an example of a successful cyber-offence. A cyber worm called 'Stuxnet'[88] was developed and released in a number of countries in 2009. The damage to computer systems caused by this attack was very minimal as compared to the damage caused in Iran. It damaged nuclear centrifuges operated in a highly-protected site at Natanz, in Iran. The damage sustained within Iran to its nuclear programme was subsequently deemed 'substantial,' and was thought to have put the nuclear weapons development programme off track for some years.[89] Stuxnet is a sophisticated weapon. It attacks and disables nuclear centrifuges that operate with a SCADA system of the Siemens type, overriding the

proprietary software and overloading the centrifuges.[90] The latter so cleverly, that it disguises the damage in progress from operators and overseers until it is too late to reverse. According to estimates it had been many months, if not years in development, with large teams of experts and access to highly restricted and classified information and equipment.

The above discussion signifies cyberspace as a domain which could be used against or to damage nuclear programmes of states, thus posing a threat to nuclear stability. The risk of sabotage of nuclear weapons systems exists in the cyber domain too. There is a possibility that attackers could send or feed wrong information into the systems and even take control of the weapons. Different parts of nuclear weapons systems are vulnerable and could be targeted during a cyber-attack. The command and control systems, alert systems, launch systems and even positioning systems could all become potential targets.

Following examples show the importance of cybersecurity and its implications for nuclear domain. In 2010, the U.S. Air Force lost computer communication with 50 Minuteman nuclear ballistic missiles for one hour, fortunately without any consequences.[91] In 2012, British researchers discovered that Chinese-manufactured computer chips used in military weapons systems, nuclear plants, etc., all over the world contain a secret "backdoor" that could facilitate disabling or reprogramming the chip remotely.[92] It is possible that such computer chips are also being used in nuclear weapons systems which could be hacked or manipulated.

Scenarios in which alert systems are hacked and show a massive nuclear attack by adversaries may lead to an accidental nuclear conflict, especially in states with

automated warning systems attached to nuclear weapons on so-called hair-trigger alert. It is also possible that hackers are able to manipulate the coordinates of targets of nuclear missiles, or to hack GPS-like systems that some missiles use to calculate their positions vis-à-vis their targets. Currently, there is no evidence that any state or non-state actor is able to successfully perform such manipulations, but considering the fast developments in the cyber arena, it might be possible in the near future. In the worst-case scenario, these possibilities may cause the unintended use of nuclear weapons, or use against unintended targets. The vulnerabilities of the nuclear weapons systems may affect nuclear stability. Especially the deterrent value of nuclear weapons may decrease, if potential adversaries think they have options to manipulate these weapons when being used. It is difficult to forecast the effects of such decreasing nuclear deterrence. Replacing nuclear weapons, cyber weapons may well become the most dangerous weapons due to their ability to manipulate, control or misuse nuclear weapons. Ultimately, this may also lead to disarmament of nuclear weapons because they may no longer be providing effective deterrence. However, there is also the possibility of using greater numbers of nuclear weapons if this is perceived as strengthening the deterrent value to some extent.

It can be argued that cyber-war is fast becoming a reality and that threats in the cyberspace are real, making it the fifth domain of warfare after land, sea, air and space. Another important aspect is the legality and conduct in the cyber domain. Being a relatively new phenomenon, the legality and conduct of cyber-warfare is still being debated and efforts are being made to devise an appropriate framework for conduct and responses in the cyber domain.

Law and Cyber-Warfare

International Law is struggling to address the issue of cyber-war, both as concerns jus ad bellum (the rules governing international armed conflict) and jus in bello (the way in which war is waged, namely international humanitarian law).[93] Questions that need clarification include whether existing international law also applies to cyber operations and, if yes, under what conditions.

Written between 2009 and 2012, the Tallinn Manual process is an effort to define norms governing cyber warfare. The manual is the most comprehensive analysis yet of how existing international law applies to cyberspace. It asserts that the general principles of international law do apply to cyberspace, including jus ad bellum and jus in bello.[94] The manual's ninety-five rules define state responsibility in cyber operations contrary to international law, applying the principle of prohibition of the use of force, the circumstances in which self-defence may be invoked, the conduct of parties during cyber hostilities, etc. It asserts that "an international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations occurring between two states or more', and that 'cyber operations alone might have the potential to cross the threshold of international armed conflict.'[95] The manual stipulates that a cyber operation can be retaliated against in self-defence, only if the conditions of a cyber armed attack ('use of force' resulting in serious physical injury and damage) are being met.[96] These rules remain open to interpretation, to the evolution of technology and cyber capabilities, as well as to criticism.

Cyber-attack as a mode of conflict raises many operational issues and, due to its inherent ambiguities, other problems as well. Foremost among these is the 'use of force' and

'act of war' dilemma.[97] There is also the problem of deterrence in cyberspace that is affecting retaliation, pre-emption, and conflict escalation. Following all the discussion and definitions of cyber-attacks, it can be argued that not every bad thing that happens in cyberspace and on the internet is war or attack. War is the use of force to cause damage, destruction or casualties for political effect by states or groups.[98] A cyber-attack may be an act intended to cause damage or destruction. Hence, there is a grey area that consists of disruption of data and services below the level of use of force. The threshold should be high for calling a disruptive activity an act of war or an attack. An act of war involves the use of force for political purposes by or against a state.[99] Force involves violence or intimidation by the threat of use of force. If there is no violence, it is not an attack. If there is no threat of violence, it is not the use of force. And here too is a grey area consisting of covert activities. However, if an attacker wants a cyber exploit to remain undetected, and if the exploit does not inflict physical damage or destruction, it is not intimidation, not the use of force, neither is it an attack.

The rules of armed conflict that guide traditional wars are derived from international treaties, such as the Geneva Conventions, International Humanitarian Law, and practices that nations consider customary international law. Among them is the UN Charter that was designed, in essence, to avoid war.[100] Article 2(4) of the Charter demands that nations "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[101] Despite reference to territorial integrity and political independence, it is now widely understood that the prohibition applies to any use of force not otherwise permitted by the terms of the Charter. It sanctions only two exceptions to this prohibition on the use of force: (1) when

the UN Security Council authorises force, and (2) when a nation acts in self-defence. Article 51 says that nothing in the Charter shall "impair the inherent right of individual or collective self-defence if an armed conflict occurs" against a UN Member. Though International Humanitarian Law does not specifically mention cyber operations, the absence of specific references to cyber-war does not mean that cyber operations are not subject to the rules of international law. The essence of an armed operation is the causation or risk of death or injury to persons and damage to or destruction of property and other tangible objects.[102] If the means and methods of cyber-war produce the same effects in the real world as conventional weapons, such as destruction, disruption, damage, injury or death, they would be governed by the same rules as conventional weapons.

Of all the legal issues regarding cyber-war, the issue of when a cyber event amounts to an act of war is most important.[103] The threshold for considering a cyber incident as the use of force is the most important debate in cyber-war. The right of self-defence is triggered by the use of force. Therefore, the question of the threshold between an act that justifies the use of force and an act that does not becomes central in cyber-war. When cyber-attacks are persistent and insidious, they could arguably pose a risk to national security if they are detrimental to industry and society as a whole; consequently affecting the security and stability of a state.[104] However, only large scale cyber-attacks on critical infrastructures that result in significant physical damage or human losses comparable to those of an armed attack with conventional weapons would entitle the victim state to invoke self-defence under Article 51 of the UN Charter.[105] While Article 2 prohibits all threats, and uses of force, Article 51 allows the use of force only in response to an armed attack. However, not all uses of force qualify as armed

attacks which are a prerequisite to an armed response. Thus, a nation may become victim of cyber force being applied against it but may not respond in kind because the force it suffered did not amount to an armed attack.

There is consensus based on international practice that propaganda, harassment, hacktivism, and crime do not justify the use of force in response. Other areas remain less clear however. For example, activities like intelligence collection or cyber probe are usually not considered sufficient justification. Non-destructive computer methodologies employed for cyber espionage may violate the domestic law of the victim nation-state but are not contrary to international law.[106] However, intelligence collection that involves the theft of terabytes of classified information – as happened with the attacks on the US Department of Defence and the US Central Command in 2008, leaving behind great damage – may eventually be interpreted as an act of war.[107] Ultimately, however, the decision about whether something is an act of war is a political one.[108]

Violation of sovereignty is an equally imprecise guide for deciding what an act of war in cyberspace is. Spies, criminals, and hackers routinely send packets across borders with malicious intent. These activities are violations of sovereignty, but individually, they do not qualify as acts of war. Inserting spies, whether physically or digitally, would not generally be regarded as a use of force justifying a forceful response. It could be argued that massive and repeated violations of sovereignty by cyber intrusions could be interpreted as acts of war. However, it would be essential for the target nation to first notify the attacker that further intrusions would be regarded as an act of war. The failure of a nation to make such a notification or complaint in the face of massive cyber intrusions over the last decade means that the

opportunity has been missed to define such a threshold or constraint in cyber conflict.[109]

Most international agreements and practices of nation-states that comprise the law of armed conflict predate the cyber era. There is an urgent need for seeking international consensus, not only on the right to response by the military, but also on rules of engagement for cyber-war, including how nations might use private-sector networks to reroute traffic and shut down attacks. While many legal tools for dealing with coordinated attacks already exist, nations need to develop policies to allow countermeasures, such as mutual aid agreements and cyber-security policies, and, foremost, for governance of cyber-war.

A defined and agreed international framework for the conduct in cyberspace is yet to be established. Even if a framework is created, it may not be enough to discourage perpetrators from conducting offences in the cyber domain. Therefore, states and organisations are concerned regarding security and defences against cyber threats and cyber-war leading to the concept of deterrence in cyber domain.

Threat Perception and Deterrence in Cyberspace (Cyber-defence)

Deterrence theory, to achieve restraint from attacks, is considered an important concept. Contemporary security studies acknowledge that limiting deterrence theory to the military, and more specifically the nuclear, domain is not viable.[110] In line with this, various authors have discussed the extent to which deterrence theory is applicable to cyberspace.

Threat perception plays a central role in developing an effective national strategy and for the purpose of applying deterrence theory. Understanding a country's or an organisation's threat assessment is crucial to understanding its strategic response. Thus, the nature of a threat, threat agents, the technical means used and the potential target are important. The European Network and Information Security Agency (ENISA), has identified six threat agents in national strategies, including corporations, cybercriminals, employees, hacktivists, nation states and terrorists.[111]

The traditional strategy of deterrence gained importance in the Cold War model of Mutually Assured Destruction (MAD) where any nuclear attack would be met with a counter nuclear strike that would also destroy the aggressor. Some scholars have tried to apply the same theoretical framework to cyberspace. Nuclear deterrence is directed primarily at nation states and, by extension, state-sponsored terrorists. It relies primarily on retaliation or punishment. However, nuclear deterrence also depends on restricting states that have nuclear arsenals and the spread of the knowledge and materials required to develop the weapons, sometimes called "deterrence by denial."[112] This in turn is supported by the establishment of international norms and agreements that limit the acquisition and use of nuclear technologies, such as the Nuclear Non-Proliferation Treaty of 1968. Scholars including Joseph Nye have even suggested an arms control framework for the cyberspace.[113]

The problem with cyber deterrence however is that it does not work as well as nuclear deterrence, because cyberspace poses certain limitations. The power of nuclear weapons compelled states towards achieving deterrence – a strategy in which the purpose of armies shifted from winning wars to preventing them. Cyber-

attacks are different as they are a means to a wide variety of political and military ends, many of which can have serious implications for national security. For example, computer hacking can be used to steal offensive weapons technologies, including weapons of mass destruction technology. Or it could be used to render adversary defences inoperable during a conventional military attack.[114] As long as secure passive cyber defence is impossible, deterrence seems the only feasible path. Attempting proactively to deter cyber-attacks may become an essential part of a country's national strategy. However, deterrence is pointless without attribution. Attribution means knowing who is attacking you, and being able to respond appropriately against the actual place that the attack is originating from.[115]

Attribution as it relates to cyber warfare is also defined as "determining the identity or location of an attacker or an attacker's intermediary."[116] In the case of a cyber-attack, an attacker's identity may be a name or an account number, and a location may be a physical address or a virtual location such as an IP address.[117] But if retaliation does not hit the attacker, he will not be deterred. And it is of legal importance as well. Retaliation against the wrong actor is unjust and a crime. Thus, attribution is a necessary condition for the law of war to be applied. An attacker needs to be identified and in order for it to be an armed attack and not just a criminal act, the attacker has to be a state actor or those acting on behalf of a state.

At the level of the nation-state, there are two possible deterrence strategies: denial and punishment. Both have three basic requirements: capability, communication, and credibility. But in cyberspace, both strategies suffer from a lack of credibility. Denial is unlikely to work due to the ease with which cyber-attack technology can be

acquired, the immaturity of international legal frameworks, the absence of an inspection regime, and the perception that cyber-attacks are not dangerous enough to merit deterrence in the first place. Punishment is a real option, but this strategy also lacks credibility due to the daunting challenges of cyber-attack attribution and asymmetry. At a minimum, attribution must improve before a cyber attacker may feel deterred. The literature on cyber deterrence reveals many challenges to this concept.[118] These include the: difficulty of attributing cyber-attacks to their perpetrators; ease of acquiring cyber weapons and conducting cyber-attacks; broad scope of state and non-state actors who engage in cyber-attacks that can be for many reasons and against both state and non-state targets; short shelf life of many cyber-weapons; difficulty of establishing thresholds and red lines for cyber aggression; difficulty of setting and enforcing international norms regarding cyber conduct; challenges associated with avoiding escalation. How to deter a cyber-attack thus remains an important question that needs to be answered.

Achieving Viable Deterrence in Cyberspace

The efficacy of cyber deterrence relies on the ability to impose or raise costs, and to deny or lower benefits related to cyber-attack in a state's decision-making calculus. Credible cyber deterrence is equally dependent on a state's willingness to use its abilities, and a potential aggressor's awareness that these abilities, and the will to use them, exists.[119]

For cyber deterrence to really work effectively, it will have to consist of a comprehensive scheme of offensive and defensive cyber capabilities, supported by a strong international legal framework. Offensive capabilities are the primary tools to impose or raise the costs in

deterrence because they provide a state the means and ways for retaliation, and enhance the perceived probability that aggressors would pay for their actions. Defensive capabilities play an equally important role in deterring cyber-attacks. Not only do they ensure that essential services and society functions continue unhindered, they also deny or lower the benefits an attacker may obtain via cyber-attacks. Defensive cyber capabilities increase a state's resistance to attacks, reduce the consequences, enable the state to strengthen the security of potential targets, and limit or eliminate an aggressor's ability to threaten the state through cyberspace. Ultimately, they reduce the probability of success that an aggressor will achieve his goals.

Apart from offensive and defensive capabilities, a strong international legal framework that addresses cyber aggression is the most critical component of a comprehensive approach to deterrence. International law and norms are fundamental to deterrence because states share an interest in adopting common standards for the conduct of international transactions, and in promoting or banning specific kinds of behaviour by states.[120] Multilateral agreements provide the most efficient way of realising these shared interests. The common acceptance of norms makes state behaviour more predictable, which leads states to insist on respect for specific norms of conduct by those who violate the code.[121]

In this way, international law builds the framework that guides how and when states employ offensive and defensive cyber capabilities, and forms the foundation for cyber deterrence. It adds to punitive actions and amplifies the costs of cyber-attack by generating a negative response from the international community. Moreover,

international law also provides a measure of protection to states that lack defensive and offensive capabilities.

There is currently "no binding international law on cyber-security expressing the common will of countries."[122] In fact, the lack of international norms to govern state behaviour in cyberspace has led to a gap that could be exploited by aggressive states.[123] For example, in response to the accusations of state-sponsored cyber-war against Estonia, the head of the Russian Military Forecasting Centre stated that "the attacks against Estonia had not violated any international agreements because no such agreements exist," suggesting that even if Russia's involvement could be proven, Estonia's diplomatic options for retaliation remained limited.[124]

The problem with cyber deterrence is that the cyber domain is still evolving. In order to practice deterrence, relevant information is lacking including the kind of damage a potential attacker would consider unacceptable. Moreover there is secrecy surrounding existing cyber-attack capabilities and their survivability for purposes of retaliation.[125] The US, China, and Russia are widely perceived to have the best capabilities, but very little is known about how they would respond to a major attack.[126] Thus, discussions about how a conflict would develop, and what it would take to deter, remain assumptions.

Another related issue is the fact that states cannot disarm cyber attackers by conducting counter cyber-attacks, and escalation cannot be avoided. In cyberspace, hackers with hidden identities could be anywhere. This means that a fight that begins in cyberspace may result in spill-over into the real world, possibly with serious consequences."[127] Responses to cyber-attacks must

weigh many factors since ambiguity in cyberspace can be used as an advantage in the event of a cyber-war.

Conclusion

Cyberspace is different from traditional domains of warfare, yet it shares many of the same characteristics as other domains. Significantly, all are domains of human practice, characterised by a wide range of activities by both state and non-state actors. Some of these activities are hard to attribute. Cyber-weapons are easily and widely available and at a relatively lesser cost and are also different in the effects they produce.

Cyber-power, in military terms, has been the most influential instrument of the past two decades. Both cyber-power and cyberspace remain at the centre of new concepts and doctrines of war. Across various levels of conflict, ranging from insurgency to main-force conventional warfare, cyber-power has become an indispensable element of modern technology-based military capability.

Cyber threats pose critical national and economic security concerns due to the rapid advances in, and increasing dependency on, Information and Communications Technology (ICT) that has been attached to the aspects of modern society. Data collection, processing, storage, and transmission capabilities are widely growing, and mobile, wireless, and cloud computing bring the full power of the globally-connected Internet to personal devices and critical infrastructures. The impact of this evolution can be seen not only in the increasing scope of cyber-security incidents, but also in the expanding range of actors and targets. Sophistication of computer network operations by both state and non-state actors has

increased in the last years. However, not all such cyber-security incidents qualify as cyber-attacks.

The availability of cyber-attack technologies for national purposes greatly expands the range of options available to national policymakers. However, it also means that their use may sometimes result in unanticipated and unintended consequences. It can be argued that cyber-warfare is a reality and cyber-attacks pose serious security challenges to the states. Since cyberspace is such a rich domain, a more focused approach is required for deterrence in cyberspace, as has been followed in traditional domains of warfare. This could be achieved by employing both defensive and offensive capabilities. Besides these capabilities, a comprehensive approach to deterrence would include a strong international legal framework that addresses cyber aggression and defines laws for conduct in cyberspace.

References

1. Carmen-Cristina Cirlig, "Cyber Defence in the EU: Preparing for Cyber Warfare?," European Parliamentary Research Service, October 2014, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2014)542143.
2. Ibid.
3. Ibid.
4. A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by blocking it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information, See: http://www.digitalattackmap.com/understanding-ddos/.
5. Andrzej Kozlowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan,"

European Scientific Journal 3, special edition (February 2014), www.eujournal.org.

6. James P. Farwell, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (February-March 2011), http://dx.doi.org/10.1080/00396338.2011.555586.
7. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 01, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=1&partner=rss&emc=rss.
8. Nicole Perlroth and Guentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.
9. "Edward Snowden: Leaks That Exposed US Spy Programme," *BBC News*, January 17, 2014, http://www.bbc.com/news/world-us-canada-23123964.
10. Ibid.
11. Ibid.
12. Paul Szoldra, "This is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks," *Business Insider*, September 16, 2016, http://www.businessinsider.com/snowden-leaks-timeline-2016-9.
13. Ibid.
14. Nir Kshetri, "Cyber-security and International Relations: The U.S. Engagement with China and Russia," Prepared for FLACSO-ISA 2014, University of Buenos Aires, School of Economics, July 2016, web.isanet.org/Web/Conferences/.../6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf.
15. Julian Borger, "Brazilian President: US Surveillance a 'Breach of International Law'," *The Guardian*, September 24, 2013, https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

16. Li Xiaokun, "China is Victim of Hacking Attacks," *People's Daily*, June 05, 2013, http://en.people.cn/90883/8271052.html.
17. Ibid.
18. Kshetri, "Cyber-security and International Relations."
19. Ibid.
20. Steve Levine, "What You Need to Know About Russia's Election Hack and Why US Senators Say It "Should Alarm Every American," *Quartz*, December 12, 2016, https://qz.com/860706/russian-hacking-and-the-us-election-why-it-matters-what-it-means-and-whats-next/.
21. Ibid.
22. "France Condemns Alleged Russian Cyber Attacks Targeting Presidential Candidate Macron," *France 24*, February 20, 2017, http://www.france24.com/en/20170219-france-condemns-cyberattacks-targeting-presidential-candidate-macron-points-russia.
23. Levine, "What You Need to Know."
24. Lizzie Dearden, "German Spy Chief Warns Russia Cyber Attacks Aiming to Influence Elections," *Independent*, May 04, 2017, http://www.independent.co.uk/news/world/europe/germany-spy-chief-russian-cyber-attacks-russia-elections-influence-angela-merkel-putin-hans-georg-a7718006.html.
25. Chris Baynes, "Vladimir Putin: Russian State Does Not Hack and Could Not Influence Foreign Elections," *EveningStandard*, May 31, 2017, http://www.standard.co.uk/news/world/vladimir-putin-russian-state-does-not-hack-could-not-influence-foreign-elections-a3554586.html.
26. Paul Cornish, "Governing Cyberspace Through Constructive Ambiguity," *Survival* 57, no. 3 (May 19, 2015), http://dx.doi.org/10.1080/00396338.2015.1046230.
27. Stefan Fenz, "Cyberspace Security: A Definition and A Description of Remaining Problems," University Vienna - Institute of Government & European Studies, October 27, 2005,

www.univie.ac.at/frisch/isegov/aushaengUniWien/CyberpaceSecurity_Fenz.pdf.

28. Joseph Nye Jr., "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no.4 (Winter 2011), http://nrs.harvard.edu/urn-3:HUL.InstRepos:8052146.
29. Ibid.
30. US Department of Defence, *Cyberspace Operations*, Joint Publication 3-12(R), The Joint Staff, November 20, 2011, www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
31. Kshetri, "Cyber-security and International Relations."
32. Fred Schreier, "On Cyberwarfare", Working Paper no. 7 (DCAF Horizon, 2015), www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf.
33. SCADA is an industrial automation control system at the core of many modern industries. Multiple software and hardware elements are deployed to monitor, gather, and process data and to connect to and control machines etc, See https://inductiveautomation.com/what-is-scada.
34. R K Tyagi, *Understanding Cyber Warfare and Its Implications for Indian Armed Forces* (India: Vij Books India Pvt Ltd, 2013), https://books.google.com.pk/books?isbn=9382573798.
35. Phil Williams and Dighton Fiddner, "Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition," United States Army War College & Strategic Studies Institute Press, Carlisle Barracks, August 2016, ssi.armywarcollege.edu/pdffiles/PUB1319.pdf.
36. Maj Gen. Mark Bar et al., "Assured Access to the Global Commons," Supreme Allied Command Transformation, North Atlantic Treaty Organisation, Norfolk, Virginia USA, April 3, 2011, www.act.nato.int/images/stories/events/2010/gc/aagc_finalreport.pdf.
37. Ibid.
38. Ibid.
39. Ibid.
40. Schreier. "On Cyberwarfare."

41. Daniel T. Kuehl, "From Cyberspace to Cyber Power: Defining the Problem," in *Cyberpower and National Security, ed.* Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Washington, DC: NDU Press/Potomac Books, Inc., 2009), ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf.
42. Anthony Craig and Brandon Valeriano eds., "Conceptualising Cyber Arms Races," (paper presented at 8th International Conference on Cyber Conflict Cyber Power, Cardiff University, Cardiff, United Kingdom, 2016), NATO CCD COE Publications, Tallinn, https://ccdcoe.org/cycon/2016/proceedings/10_craig_valeriano.pdf.
43. John Arquilla, "Cyberwar Is Already Upon Us." *Foreign Policy*, Feb 27, 2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us.
44. Kuehl, "From Cyberspace."
45. John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* (Summer 2011), www.au.af.mil/au/ssq/2011/summer/sheldon.pdf.
46. Franklin D Kramer, Stuart H star and Larry K Wentz eds., *Cyber Power and National Security* (Washington DC: National Defence University Press, Potomac Books Inc, Virginia, 2009).
47. Joseph Nye, "Cyber Power."
48. Kramer, *Cyber Power and National Security*.
49. Ibid.
50. Schreier. "On Cyberwarfare."
51. Cirlig, "Cyber Defence."
52. Ibid.
53. Office of the Vice Chairman of the Joint Chiefs of Staff, Memorandum for the Chiefs of the Military Services, Joint Terminology for Cyberspace Operations, Washington D.C., 2010-2011, www.nsci-va.org.
54. See: http://definitions.uslegal.com/c/cyber-warfare/.
55. bid.

56. Shane M. Coughlan, "Is There a Common Understanding of What Constitutes Cyber Warfare?," The University of Birmingham, School of Politics and International Studies, September 30, 2003, 2, www.opendawn.com/cyber-warfare/.
57. Office of the Vice Chairman of the Joint Chiefs of Staff, Memorandum for the Chiefs of the Military Services, Joint Terminology for Cyberspace Operations, Washington D.C., 2010-2011, www.nsci-va.org.
58. Ibid.
59. Stephen A. Hildreth, "Cyberwarfare," Congressional Research Service Report for Congress no. RL30735, June 19, 2001, https://fas.org/sgp/crs/intel/RL30735.pdf.
60. Office of the Vice Chairman of the Joint Chiefs of Staff, Memorandum for the Chiefs of the Military Services, Joint Terminology for Cyberspace Operations, Washington D.C., 2010-2011, www.nsci-va.org.
61. Kevin Coleman, "The Cyber Arms Race Has Begun," CSO Online, January 28, 2008, http://www.csoonline.com/article/2122353/critical-infrastructure/coleman--the-cyber-arms-race-has-begun.html.
62. UN Security Council, Resolution 1113 (2011), 5 March 2011.
63. James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism* (New York: Citadel Press, 2002), 11.
64. Ibid.
65. James A. Lewis & Katrina Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organisation," UNIDIR Resources, Centre for Strategic and International Studies, 2011, http://unidir.org.
66. Christian M. Cupp and Phyllis Levine, "Information Terrorism," DTIC Review 5, no. 1 (March 2000), https://www.hsdl.org/?view&did=438670.
67. ICT is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems etc, See: www.igi-

global.com/dictionary/information-and-communication...icts/14313.

68. CNO is a broad military computing concept that encompasses tools, processes and methodologies to utilise, optimise and gain strategic advantages from computer networks, See: https://www.techopedia.com/definition/27907/computer-network-operations-cno.
69. Office of the Vice Chairman of the Joint Chiefs of Staff, Memorandum for the Chiefs of the Military Services, Joint Terminology for Cyberspace Operations, Washington D.C., 2010-2011, www.nsci-va.org.
70. Myriam D Cavelty, "Cyberwar: Concept, Status quo, and Limitations," *Policy CSS Analysis in Security Policy*, CSS ETH Zürich no. 71 (April 2010), 2, www.css.ethz.ch/publications/pdfs/CSS-Analyses-71.pdf.
71. Ibid.
72. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, Project Air Force, 2009), www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.
73. Ibid.
74. Ibid.
75. Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4, no. 63 (2010). http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.
76. Ibid.
77. Ibid.
78. Ibid.
79. Libicki, *Cyberdeterrence and Cyberwar*.
80. Ibid.
81. Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (US: Harper Collins, 2010).
82. David A. Fulghum, "Searching for Ways to Trace Cyber Attackers," *Aviation Week and Space Technology* (May 20, 2011).

83. A "bot" is a type of malware that allows an attacker to take control over an affected computer. Also known as "Web robots", bots are usually part of a network of infected machines, known as a "botnet", which is typically made up of victim machines that stretch across the globe. See: https://us.norton.com/botnet/
84. Libicki, *Cyberdeterrence and Cyberwar*.
85. Fulghum, "Searching for Ways."
86. John Palfrey et al., "2010 Report on Distributed Denial of Service (DDoS) Attacks," Berkman Klein Centre for Internet & Society at Harvard University, https://cyber.harvard.edu/publications/2010/DDoS_Independent_Media_Human_Rights.
87. Ibid.
88. Stuxnet is a computer worm that targets industrial control systems that are used to monitor and control large scale industrial facilities like power plants, dams, waste processing systems and similar operations. It allows the attackers to take control of these systems without the operators knowing. See: https://us.norton.com/stuxnet
89. Shreeya Sinha and Susan Beachy, "Timeline on Iran's Nuclear Programme," *The New York Times*, https://www.nytimes.com/interactive/2014/11/20/world/middleeast/Iran-nuclear-timeline.html?mcubz=1&_r=0
90. CRS Report for Congress, Congressional Research Service, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability, by* Paul K. Kerr, John Rollins and Catherine A. Theohary, R41524 (December 9, 2010), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-040.pdf.
91. Larry Shaughnessy and Chris Lawrence. "Air Force Lost Some Communication With Nuclear Missiles." *CNN News*, October 27, 2010, http://edition.cnn.com/2010/US/10/26/nukes.lost.communications/.
92. Sophie Curtis. "Cambridge Researchers Uncover Backdoor in Military Chip," *Techworld*, May 29, 2012, http://www.techworld.com/news/security/cambridge-researchers-uncover-backdoor-in-military-chip-3360617/.

93. "Jus in Cyber Bello: How the Law of Armed Conflict Regulates Cyber Attacks Part I," INFOSEC Institute, April 2014, http://resources.infosecinstitute.com/jus-cyber-bello-law-armed-conflict-regulates-cyber-attacks-part/#gref.
94. Dr. Alireza Hojatzadeh and Afshin Jafari, "Cyber-attacks and Jus Ad Bellum," *International Journal of Humanities & Social Science Studies* 1, no. 2 (September 2014), https://www.ijhsss.com/files/Afshin-Jafari_u7kn99r3.pdf.
95. Michael Schmitt, "Classification of Cyber Conflict," *Journal of Conflict and Security Law* 17, no. 2 (Summer 2012), https://academic.oup.com/jcsl/article/17/2/245/.../Classification-of-Cyber-Conflict?rss=1.
96. Ibid.
97. Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack," Yale Law School, Faculty Scholarship Series Paper 3852, 2012, http://digitalcommons.law.yale.edu/fss_papers/3852.
98. James A. Lewis, "Thresholds for Cyberwar," Report, Centre for Strategic and International Studies, September 2010, https://www.csis.org/analysis/thresholds-cyberwar.
99. Ibid.
100. Matthew Hoisington, "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defence," *Boston College International and Comparative Law Review* 32, no. 2 (2009). http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1115&context=iclr.
101. UN Charter, Chapter 1 Article 2(4), http://www.un.org/en/sections/un-charter/chapter-i/.
102. Hathaway and Crootof, "The Law of Cyber-Attack."
103. Gen. Charles J. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* (Spring 2011), http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2992&context=faculty.
104. Schreier, "On Cyberwarfare."
105. Marco Roscini, "World Wide Warfare – 'Jus Ad Bellum' and the Use of Cyber Force," *Max Planck Yearbook of*

United Nations Law 14 (September 2010), https://ssrn.com/abstract=1683370.

106. Walter Sharp, *Cyberspace and the Use of Force* (San Antonio: Aegis Research Corp., 1999), www.thomas-hastings.org.

107. "Cyber War: Sabotaging the System," *CBS News*, *November* 2009, http://www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/.

108. Libicki, "Cyberdeterrence and Cyberwar," Annex A: What Constitutes an Act of War in Cyberspace?.

109. In May 2011, the Pentagon decided that cyber-attacks constitute an act of war. In a classified document it concluded that the US may respond to cyber-attacks from foreign countries with traditional military force, See: Cyber Combat: Act of War, *The Wall Street Journal*, May 31, 2011, https://www.wsj.com/articles/SB10001424052702304563104576355623135782718.

110. Annegret Bendiek and Tobias Metzger, "Deterrence theory in the cyber-century," Research Division EU/Europe
Stiftung Wissenschaft und Politik German Institute for International and Security Affairs, May 2015, https://subs.emis.de/LNI/Proceedings/Proceedings246/553.pdf.

111. European Union Agency for Network And Information Security, ENISA Threat Landscape 2015, https://www.enisa.europa.eu/publications/etl2015/at_download/fullReport.

112. Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," Centre for Security Studies, ETH Zurich Department of Humanities, Social and Political Sciences, April 22, 2013, https://www.ethz.ch/content/specialinterest/gess/cis/center-for.../en/.../190088.

113. Joseph Nye, "The World Needs New Norms on Cyber-warfare," *The Washington Post*, October 1, 2015, https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-

cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html?utm_term=.6f1566cbca11.

114. David A. Fulghum, Robert Wall & Amy Butler, "Cyber-Combat's First Shot," *Aviation Week & Space Technology* 167, November 26, 2007.

115. Gen (R) Ron Keys, Charles Winstead and Kendra Simmons, "Cyberspace Security and Attribution," National Security Cyber Space Institute NSCI, July 20, 2010, http://www.nsci-va.org/WhitePapers/2010-07-20-Cybersecurity%20Attribution-Keys-Winstead-Simmons.pdf.

116. Ibid.

117. David A. Wheeler, "Techniques for Cyber Attack Attribution," Institute for Defence Analyses, IDA Paper P-3792, October 2003, www.dtic.mil/dtic/tr/fulltext/u2/a468859.pdf.

118. Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," *Military and Strategic Affairs* 3, no. 3 (December 2011), http://i-hls.com/wp-content/uploads/2013/02/Cyber-Warfare-and-Deterrence.pdf.

119. Schreier, "On Cyberwarfare."

120. Charles W. Freeman, *Diplomatic Strategy and Tactics in Arts of Power* (Washington D.C.: US Institute for Peace, 1997), 84, https://bookstore.usip.org/sites/usip/resrcs/chapters/1878379658_otherchap.pdf.

121. Ibid.

122. Ministry of Defence, Estonia, Cyber Security Strategy, Tallinn, 2008, https://www.unodc.org/res/cld/lessons-learned/cyber-security-strategy_html/Cyber_Security_Strategy_Estonia.pdf.

123. Eneken Tikk et al., "Georgian Cyber Attacks: Legal Lessons Identified," Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2008, www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf.

124. Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala*

8, no. 1 (October 2008), 51, www.international-relations.com/CM8-1/Cyberwar.pdf

125. Schreier, "On Cyberwarfare."
126. Ibid.
127. Libicki, "Cyber deterrence and Cyberwar."