Istituto Affari Internazionali

ISSN 2280-6164

DOCUMENTI IAI 18 | 03 - MARCH 2018

Non-proliferation Regime for Cyber Weapons. A Tentative Study

by Cristian Barbieri, Jean-Pierre Darnis and Carolina Polito

ABSTRACT

Conflicts today are no longer confined to the three conventional areas of warfighting – land, sea, and air. Cyber space is now increasingly being recognized as a fourth area of conflict, with countries incorporating cyber elements into their traditional military doctrines, or developing offensive cyber capabilities and cyber military commands. As cyber space becomes more militarized, we are also increasingly seeing nation-state or state-sponsored cyber-attacks rise. Difficult to trace and shrouded in anonymity, how can the world address the potential risks of cyber weapons proliferation? What kind of agreement could be reached to prevent cyber conflict with these new capabilities? What role can confidence building measures or cyber norms play in de-escalation? This paper provides an analysis on the cyber weapons proliferation debate, leveraging the lessons learned from past international agreements, and offering a potential way forward to ensure that an open, stable, and secure cyber space remains.

keywords

Cyber-security | WMD | Non-proliferation | International humanitarian law | Treaties

Non-proliferation Regime for Cyber Weapons. A Tentative Study

by Cristian Barbieri, Jean-Pierre Darnis and Carolina Polito*

Introduction

Conflicts today are no longer confined to the three conventional domains of land, sea, and air. The attacks to network and information systems that form part of the cyber domain have increased to such an extent that these attacks present issues for international peace and security and are now a major element of discussion at the highest levels of international government and industry. Governments around the world are prioritizing the development of offensive and defensive cyber capabilities.

The last few years have witnessed a proliferation of headline-grabbing cyber-attacks perpetrated both by organized crime groups seeking financial gain, as well as nation-states who are increasingly using cyber-attacks as means to extend their geopolitical reach. The impact of the Stuxnet worm, Wannacry ransomware, and alleged Russian state-sponsored attacks in Georgia and Estonia, are just some examples of the level of damage that cyber weapons can achieve.

Since the cyber domain is characterized by unique features such as ubiquity, speed, absence of political or geographic boundaries, as well as the ability to accumulate large bodies of information over long distances in real-time, international administrations, national governments, and the private sector are now faced with unprecedented security issues.

Based on the features of the cyber domain, cyber weapons are posing serious challenges for public and private sector alike. Key issues include: attribution of cyber actions; the dual-use nature of cyber weapons; unpredictability and potential for collateral damage; and the ability to use cyber weapons as a force multiplier for conventional military operations.

* Cristian Barbieri is Junior Researcher at the Istituto Affari Internazionali (IAI). Jean-Pierre Darnis is Scientific Advisor and Head of the Tech-IR Programme at IAI. Carolina Polito studies International Relations at the University of Bologna and has been an intern at IAI.

· Paper prepared for the Istituto Affari Internazionali (IAI), March 2018. Presented at the debate on "A Non-proliferation Regime for Cyber Weapons?" organized by IAI and Microsoft in Brussels on 19 March 2018. This study has been conducted with the support of Microsoft. The analysis and opinions expressed herein are solely those of the authors.

ISSN 2280-6164

Recent developments at the international level suggest, however, that there might be an emerging consensus among states in favour of agreed rules governing the cyber arena. In addition, across the tech sector, companies are increasing the cyber security protection they provide for consumers worldwide.

Within the community of experts and analysts several questions remain at the core of cyber weapon control, including: (1) Is the world experiencing a cyber arms race? (2) Is an arms control regime in the cyber arena really needed? (3) Can other international treaties serve as examples in the creation of an international organization for cyber issues? (4) What is the state of play of international agreements in the cyber field? (5) How can an international cyber treaty deal with the more challenging cyber weapons features, such as unpredictability, accountability and attribution?

This study, while aware that most of the questions raised can only be partially addressed, aims to contribute to the debate on cyber conflict and the cyber arms race. By drawing from lessons learned from past treaties in other domains and the various ongoing initiatives in the cyber field, the final goal will be to understand the opportunities and challenges that would need to be overcome by a future international treaty on cyber weapons.

The study opens with a context assessment which focuses on the definitions of key terms and a strategy description of the main actors' cyber capabilities. To date, there has not been international consensus over the definitions of key terms, such as what constitutes a cyber-attack. Thus, this section will try to clarify and distinguish some of these terms.

The second chapter will address existing arms control regimes such as the Biological Weapons Convention (BWC), the Chemical Weapons Convention (CWC) and the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) from which we can draw important policy lessons and elements to be potentially applied to the field of cyber space.

Previous policy activities by international organizations in the cyber domain have not yet achieved global consensus. The United Nations Group of Governmental Experts (UNGGE), the European Union initiatives towards cyber security, the NATO public private partnerships, the Shanghai Cooperation Organization proposal for an international code of conduct on information warfare, the confidence-building measures put in place by the Organization for Security and Co-operation in Europe (OSCE) and the Wassenaar Arrangement, are the focus of the third chapter. Even though these actions by international organizations prepare the ground for further multilateral and multi-stakeholder initiatives in the cyber domain, the debate is still open and must be fostered.

The issues of attribution, verification, the threshold for recognizing a cyber-attack as a "use of force" or "armed conflict" under international humanitarian law, active defence, dual-use and segregation of civilian and military infrastructures, the role

ISSN 2280-6164

of private sector experts, and confidence building measures are just some of the issues which are resumed in the last chapter. The goal is to outline these issues and present them in the context of international law, the Geneva conventions, and the analogue arms control treaties that are analysed in the second chapter as well as in the context of the international cyber initiatives discussed in the third chapter.

Finally, the conclusion will summarize the study and provide guidelines for a future international cyber agreement.

1. Definitions and actors

1.1 Definitions

The narrative on "cyber space" and "cyber security" is vast and unfocused. Experts approaching the issue come from a variety of backgrounds, using different terms to define the concept, and in some situations definitions may even vary from country to country. The US Government, for example defines cyber space as "[a] global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"[1] – whereas cyber security usually refers to the protection of confidentiality, integrity and availability of data. Others take a broader view, for example, the Russian government refers to cyber space as "information space" and to cyber security as "information security" in order to also include issues related to online content. Several efforts have been undertaken to help produce a more common vocabulary based on globally accepted definitions across a variety of disciplines such as law, international relations and even within the cyber security community. As this field is continuously evolving, globally accepted definitions – either do not exist or are only slowly developing.

The use of the term "cyber warfare" is particularly complex. Many argue that the term has been either overused or applied to contexts (including some of the more sophisticated cyber-attacks in recent years) that, from an international relations and/or legal perspective, would not justify using the term "war".[2] In fact, cyber war is often an abuse of the more general spectrum of action in cyber space, which should be well divided, and not be confused with other kinds of nefarious activities such as cyber espionage, cybercrime, or cyber-enabled acts of terrorism. The media bears a major responsibility in the confusion around these terms. The media usually labels "cyber warfare" as anything that would more appropriately be limited

[1] Richard Kissel (ed.), "Glossary of Key Information Security Terms", in *NIST Interagency/Internal Report (NISTIR)*, No. 7298rev2 (May 2013), p. 58, https://www.nist.gov/node/579721.

[2] For more on the definition of cyber war see inter alia Joseph S. Nye Jr., *The Future of Power*, New York, PublicAffairs, 2011; John Stone, "Cyber War Will Take Place!", in *Journal of Strategic Studies*, Vol. 36, No. 1 (2013), p. 101-108; and Richard A. Clarke and Robert K. Knake, *Cyber War. The Next Threat to National Security and What to Do about It*, New York, HarperCollins, 2010.

ISSN 2280-6164

to cyber conflict or cyber espionage. This study will use the term "cyber offensive capabilities and/or actions" instead of "cyber warfare" following the reasoning of Valeriano and Maness, which affirms that "the term cyber war is overwrought and descriptive of a process that has yet to occur".[3] Of course, there is no clear-cut definition of when cyber conflict becomes a cyber warfare scenario.

Given the need for further clarification over these important terms, it becomes important to define the environment in which a cyber conflict would be fought, which is cyber space. Despite being a relatively new method of conflict, the term "cyber space" has been referred to in official government documents for nearly a decade. Following the 2007 cyber-attacks against critical infrastructures in Estonia, and many subsequent examples of state sponsored cyber-attacks, many national security strategies started to include the cyber domain. The idea that a clearer codification was needed also started to spread amongst international relations experts. From research conducted on the national security strategies of the members of the United Nation Security Council, and from various international agreements, there appears to be a lack of consensus around the terminology.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), based in Tallinn, has tried to develop a series of definitions in the Tallinn Manual, which many experts consider "the most comprehensive analysis of how existing international law applies to cyber space".[4] The Tallinn Manual defines cyber space as "The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks".[5] The definition offered by the group of experts who authored the manual, in fact, contributes to the understanding of the issue by also mentioning the physical part of the machines. When speaking about cyber space, it is always important to keep in mind that every piece of data, every action and every interaction are located and happening somewhere physically in the world. This specification is crucial and should be kept in mind in defining any scenario of application of an international control regime, mainly because it entails the problem of attribution. Thus, the main characteristics of cyber space are the union between a non-physical space and a physical one, the presence of information data, networks and the possibility to act on this data remotely.

Given the absence of internationally recognized definitions for the term "cyber space", we cannot expect a common definition of cyber warfare. Different perspectives on the matter have been adopted by national administrations in official white papers on defence, and by scholars and researchers. The first clash is

[3] Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities. Cyber Conflict in the International System*, Oxford, Oxford University Press, 2015, p. 31.

[4] Atlantic Council, *International Law and Cyber Operations - Launch of the Tallinn Manual 2.0*, Washington, 8 February 2017, http://www.atlanticcouncil.org/events/detail/international-law-and-cyber-operations-launch-of-the-tallinn-manual-20.

[5] Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, Cambridge University Press, 2017, p. 564.

DOCUMENTI IAI 18 | 03 - MARCH 2018
ISSN 2280-6164

one of terminology, which creates a deep difference in the concept of cyber space between China, Russia and the Western powers. China and Russia refer to cyber space, and subsequently to cyber warfare, as respectively "information space" and "information warfare".

In 2011, through the Shanghai Cooperation Organization, an international organization formed by eight states and predominantly led by Russian and Chinese administrations, Russia proposed an International Code of Conduct for Information Security to the UN General Assembly.[6] In addition to the SCO's joint proposal, Russia has developed a draft Convention on International Information Security.[7] This proposal contained the information space and information warfare definitions. Information space was defined as "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself". This definition has some similarities to the Western idea of cyber space, aside from the focus on the effects on individual and social consciousness. The idea of a social sphere within the data and information shared on the "space", physical or not, is persistent also in the definition of "information warfare" which states: "conflict between two or more States in the information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents".

The terms "information space" and "information war" have been used since the nineties in Western countries as well. The reasons why a change of paradigm occurred in these countries may be linked to a necessity of constraining the use of the term; the Russian convention proposal on information security was rejected by the United States and many European countries at the time because it was seen as an attempt to control free speech and online content.

Due to this absence of international legal frameworks for cyber conflict and the doctrinal divisions around the term cyber warfare, this study attempts to build off of the Tallinn Manual. The manual raises awareness that cyber warfare is too limited a concept to deal with what happens in the cyber domain, and therefore

[6] UN General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* (A/66/359), 14 September 2011, http://undocs.org/A/66/359.

[7] Russia's Ministry of Foreign Affairs, *Convention on International Information Security*, 22 September 2011, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666. See also Keir Giles, "Russia's Public Stance on Cyberspace Issues", in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds.), *4th International Conference on Cyber Conflict. Proceedings 2012*, Tallinn, NATO CCDCOE, 2012, p. 63-75, http://www.ccdcoe.org/node/378.html.

ISSN 2280-6164

cyber offensive operations is a more appropriate term. To facilitate comprehension of the terms "cyber offensive actions", "cyber-attacks", and "cyber operations" will be interchangeable throughout the study.

1.2 Key actors

This study focuses attention on official, national cyber strategies and offensive cyber capabilities within the military or intelligence components of governments. It will not address hybrid groups, such as Anonymous, or terrorist groups using cyber capabilities.

In the last decade, nation states have been increasingly concerned about the threats in cyber space, including nation-state or state-sponsored attacks and cybercrime. Therefore, cyber command units have been created with both defensive and offensive purposes. On 14 June 2016, NATO defence ministers recognized cyber space as the fifth operational military domain.

Around the world, from developed- to emerging-market countries, nations are investing in offensive capabilities. Some reports estimate that around 30 countries have offensive cyber capabilities, however, those developing capabilities covertly is likely to be much higher.[8] The following section analyses a few of the main cyber threat actors, namely, the United States, China, Russia and several European Union member states. While we recognize that there are other nation states acquiring offensive cyber capabilities such as Israel, Iran and Syria, we have chosen to focus on those mentioned above.

The **United States** is considered to be the leading superpower in terms of cyber capabilities. They have been actively developing their capabilities (both defensive and offensive) for the past two decades, and their capabilities appear to be far ahead of other countries.[9] In order to improve US cyber defence, in 2010 the United States Cyber Command (USCYBERCOM) was formed, centralizing defensive and offensive cyber space operations under the US Strategic Command. USCYBERCOM aims to ensure freedom of action in cyber space for the US government and its allies, and at the same time deny that possibility to adversaries. The service elements of the USCYBERCOM are the Army Cyber Command, the Fleet Cyber Command, the Air Force Cyber Command and the Marine Forces Cyber Command.

In addition to the standalone combatant command, there are numerous additional programmes funded by the Department of Defence in order to research and develop cyber warfare capabilities, such as the Defence Advanced Research Project Agency

[8] James R. Clapper, Marcel Lettre and Michael S. Rogers, *Foreign Cyber Threats to the United States*, Joint Statement for the Record to the Senate Armed Services Committee, 5 January 2017, https://www.armed-services.senate.gov/download/clapper-lettre-rogers_01-05-17.

[9] Jennifer Valentino-DeVries, Lam Thuy Vo and Danny Yadron, "Cataloging the World's Cyberforces", in *The Wall Street Journal*, 28 December 2015, http://graphics.wsj.com/world-catalogue-cyberwar-tools.

ISSN 2280-6164

(DARPA) programme Plan X. The project has been developed in response to the US Army's need to improve its ability to respond to more advanced cyber-attacks. The programme merges military and computer science research in cyber space. In fact, its goal is to unify the architecture from which to conduct cyber operations and allow operators to visualize cyber terrain, so that any threat can be immediately recognizable.[10] The goal of Plan X is to create a user-friendly programme, in which operators can apply military techniques in cyber space. Notably, in September 2014, the Army allocated an additional 20 million dollar worth of funds to supplement their initial 120 million dollar contract.[11] While DARPA has explicitly stated it will not develop cyber offensive capabilities, once the research is shared, policymakers may choose to use these capabilities for alternative purposes.[12]

Many cyber operation specialists in the US Army are specifically prepared to conduct both defensive and offensive operations, such as protect data and networks or targeting and responding to hostile attacks. Other specialized cyber operational expertise also exists across a range of government departments and agencies such as the National Security Agency and the Central Intelligence Agency.

The increasing effort to operationalize US cyber capabilities has also been displayed by the latest developments in its cyber strategy. During President Donald Trump's campaign, he expressed his willingness to guarantee American dominance in the field. Accordingly, in August 2017 the United States Cyber Command was elevated to the status of a Unified Combatant Command,[13] which effectively strengthens its role, resources and capabilities. Moreover, the National Defence Strategy for 2018, states that the US government will prioritize the integration of cyber capabilities into the full spectrum of military operations.[14]

China is also considered one of the most prominent cyber power in the world. The most recent Chinese military strategy is outlined in an official Information Office of the State Council White Paper published in May 2015.[15] Chinese policymakers define cyber space as "new commanding heights in strategic competition". They are keenly aware of the military transformations that are occurring in the international arena, and they believe that those revolutionary changes in military

[10] Cheryl Pellerin, "DARPA's Plan X Gives Military Operators a Place to Wage Cyber Warfare", in *DoD News*, 12 May 2016, https://www.defense.gov/News/Article/Article/758219.

[11] Morgan Cole, "Army Turns to Plan X to Defend against Cyber Threats", in *Defense Systems*, 20 September 2017, https://defensesystems.com/articles/2017/09/20/army-cyber-defense-darpa-plan-x.aspx.

[12] See DARPA website: *Plan X*, https://www.darpa.mil/program/plan-x.

[13] White House, *Statement by President Donald J. Trump on the Elevation of Cyber Command*, 18 August 2017, https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command.

[14] US Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, January 2018, p. 6, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[15] China's Ministry of National Defense, *China's Military Strategy*, May 2015, http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm.

ISSN 2280-6164

technologies "not only had a significant impact on the international political and military landscapes, but also posed new and severe challenges to China's military security".

Therefore, to be able to respond to a severe cyber-attack in 2011 the Online Blue Army was established, with a 10-million-yuan (about 1.5 million dollars) budget at their disposal.[16] The aim was to protect network security and enhance the level of information about cyber threats. In 2013 however, China publicly admitted that it had cyber units not only for defence, but also for offensive purposes. In an updated edition of *The Science of Military Strategy*, Chinese officials acknowledged that within the People's Liberation Army (PLA), it has "specialized military network warfare forces".[17]

Mandiant, a US cyber security firm, has investigated computer security breaches at hundreds of organizations, attributing many of these breaches to the organization known as Advanced Persistent Threat 1 (APT1). In 2013, Mandiant released a report in which they provided technical attribution demonstrating that APT1 originated in China.[18] Their report points out that APT1 is similar in mission, capabilities and resources to a unit within the PLA, called Unit 61398. Mandiant uncovered further evidence which demonstrated that several attacks targeting American corporations and government agencies were launched from locations that corresponded precisely to the headquarters of PLA Unit 61398. In May 2014, five members of PLA Unit 61398 were formally indicted by the American government as responsible for hacking into the networks and copying e-mails of Westinghouse Electric, the United States Steel Corporation, and of other US companies.[19]

Russia is another threat actor which is widely recognized to have sophisticated offensive cyber capabilities. Russia recognizes cyber conflict as under the umbrella of information warfare, which includes intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems and propaganda.[20] The goal of Russia's information warfare campaigns is to control information.

The first, large-scale and coordinated use of Russia's cyber capabilities to affect a strategic outcome in a neighbouring state, allegedly occurred during the

[16] Hannah Beech, "Meet China's Newest Soldiers: An Online Blue Army", in *Time*, 27 May 2011, https://wp.me/p1lnq5-1fy.

[17] Joe McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy", in *China Briefs*, Vol. 15, No. 8 (17 April 2015), p. 4, https://jamestown.org/?p=12824.

[18] Mandiant, *APT 1. Exposing One of China's Cyber Espionage Units*, February 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[19] Michael S. Schmidt and David E. Sanger, "5 in China Army Face U.S. Charges of Cyberattacks", in *The New York Times*, 19 May 2014, https://nyti.ms/2FDiqQm.

[20] David J. Smith, "How Russia Harnesses Cyberwarfare", in *AFPC Defense Dossier*, No. 4 (August 2012), p. 7-8, http://www.afpc.org/files/august2012.pdf.

ISSN 2280-6164

distributed denial of services (DDoS) attacks against Estonia in 2007. The DDoS attack flooded the web servers of several Estonian critical infrastructure providers, including some in the financial services industry.

The Russia-Georgia war in 2008 is considered to be one of the first kinetic conflicts that included a cyber offensive component. During this conflict, Georgian government websites were targeted and in some cases, completely taken offline effectively severing communications capabilities. Following the conflict with Georgia, Russia established new "Information Troops" in charge of cyber operations within the Russian Army.[21] More recently, Russia was believed to have been involved in cyber operations known as the BlackEnergy attack during its conflict in eastern Ukraine.

Finally, in 2013 the Russian Government announced its intention to create a new cyber unit, the Foundation for Advanced Military Research, in charge of offensive and defensive cyber operations, as well as a cyber research and development agency, similar in purpose to the American DARPA.[22] The Foundation has three areas of military research and development – futuristic weapons, future soldier equipment and cyber warfare.[23]

A peculiar characteristic of Russian cyber offensive capabilities is the loose connection between the government and hacktivists and criminal organizations. While any direct connection or sponsorship is yet to be proven, this symbiotic relationship would have reason to continue due to the ability of the government to maintain plausible deniability through using proxy groups, thereby extending protections to such groups operating within the government's jurisdiction.[24]

Within Europe, the **United Kingdom** is one of the leading cyber powers.[25] It operates through different national organizational structures for cyber security and cyber defence. As early as 2012, the British Joint Cyber Forces Command, a part of the Ministry of Defence, began to take the lead in the development and integration of cyber defence capabilities.[26]

[21] Keir Giles, "'Information Troops' – a Russian Cyber Command?", in Christian Czosseck, Enn Tyugu and Thomas Wingfield (eds.), *3rd International Conference on Cyber Conflict. Proceedings 2011*, Tallinn, NATO CCDCOE, 2011, p. 45-60, https://ccdcoe.org/node/375.html.

[22] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare", in *CNA Occasional Papers*, March 2017, p. 8, https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

[23] Andrew Jones and Gerald L. Kovacich, *Global Information Warfare. The New Digital Battlefield*, 2nd ed., Boca Raton, CRC Press, 2016, p. 46.

[24] David J. Smith, "How Russia Harnesses Cyberwarfare", cit.

[25] James Andrew Lewis and Götz Neuneck, *The Cyber Index. International Security Trends and Realities*, New York and Geneva, United Nations, 2013, http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

[26] UK House of Commons Defence Committee, *Defence and Cyber-security. Written Evidence*, February 2012, https://publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/1881.pdf.

ISSN 2280-6164

The cyber security national budget was increased from 860 million pounds in 2011-2016 to 1.9 billion pounds in 2016-2021,[27] which reflects a clear prioritization of cyber security issues by the government. In addition, the UK Cyber Security Strategy (2016-2021) explicitly acknowledges its offensive cyber capabilities. Such measures include intrusion into an opponent's networks with the intention of causing damage, disruption or destruction.[28] The report underlines, among other things, the significant threat of state sponsored cyber-attacks.

The UK position on the use of offensive cyber capabilities can be discerned from recent statements by British cabinet officials such as the Defence Minister. In a statement on 27 June 2017, Sir Michael Fallon said that a reaction against a cyber-attack could eventually include responses from any other domain and that "we are making sure that offensive cyber is an integral part of our arsenal".[29]

Similar statements have been made by other representatives of the UK government, including by Foreign Secretary Boris Johnson. During a meeting with his Russian counterpart, Sergey Lavrov, in Moscow on 22 December 2017, Johnson said that the UK possesses sufficient capability to serve as a deterrent to potential cyber-aggressors, and that the Russians were responsible for numerous cyber-attacks against the West.[30]

France has also acknowledged cyber threats as a great concern for national security. In 2013, in response to the increasing challenges in cyber space, intensified by globalization, the French government released a new white paper, in which it recognized "For the first time, the armed forces model includes military cyber defence capabilities, in close liaison with intelligence and defensive and offensive planning, in preparation for or support of military operations".[31]

In January 2017, the French Cyber Defence Command Unit (*Commandement de Cyberdéfense*, COMCYBER) was created. The COMCYBER will incorporate 2,600 agents by 2019, of which 600 will be computer experts from the Directorate General for Armament (DGA) who will focus on cyber offensive capabilities.[32] This new

[27] UK Government, *National Security Strategy and Strategic Defence and Security Review 2015*, November 2015, p. 40, https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

[28] UK Government, *National Cyber Security Strategy 2016-2021*, November 2016, p. 51, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

[29] UK Ministry of Defence, *Defence Secretary's speech at Cyber 2017 Chatham House Conference*, 27 June 2017, https://www.gov.uk/government/speeches/defence-secretarys-speech-at-cyber-2017-chatham-house-conference.

[30] Andrew Woodcock, "Boris Johnson Tells Russia to Halt Cyber Attacks on the West during Visit to Moscow", in *The Indipendent*, 22 December 2017, http://www.independent.co.uk/news/uk/politics/boris-johnson-russia-latest-cyber-attacks-putin-moscow-a8123681.html.

[31] France Government, *French White Paper on Defence and National Security 2013. Twelve Key Points*, July 2013, p. 5, http://www.defense.gouv.fr/actualites/articles/livre-blanc-2013.

[32] Gil Bousquet, "Paris et Berlin déploient leurs cyber-soldats", in *La Dépêche*, 17 December 2016, https://www.ladepeche.fr/article/2016/12/17/2481004-paris-et-berlin-deploient-leurs-cyber-

ISSN 2280-6164

centralized command will enable France to leverage flexible and quick response options, including the possibility of offensive options, such as techniques to neutralize or breach an enemy's systems.[33] According to the Military Planning (2014-19) Act,[34] in the coming years, France will likely invest one billion euros for cyber defence, including 450 million euros for research and equipment, and 3,200 job positions in cyber defence.[35]

In addition to the United Kingdom and France, other European countries are also updating their national cyber security strategies, to reflect the increasing importance of cyber security. Both **Germany** and **Italy**, for example, have recently built cyber commands unit into their national armies. In response to several prominent cyber-attacks, in April 2017, Germany formed a new 13,500-person cyber operations branch within the military, the Cyber and Information Space Command (CIR).[36] It is responsible for the protection of the Bundeswehr's computer networks and weapons systems, and the development of cyber offensive capabilities. The Cyber and Information Space Command's structure is divided into three units: the Strategic Reconnaissance Command, the Geo Information Centre and the IT Command.[37]

Similarly, Italian awareness of cyber security issues has also significantly grown over the past few years. To actively respond to cyber threats, including those perpetrated by nation-state or state-sponsored actors, the Italian Ministry of Defence established a Joint Cyber Command (*Comando Interforze per le Operazioni Cibernetiche*, CIOC).[38] The main domains of the unit's actions will be the defence of Italian networks, the strengthening of cyber defence capabilities, as well as the planning and executing of computer network operations. The development of offensive cyber capabilities has not been specifically outlined as an objective.

soldats.html.

[33] Tom Reeve, "France Unveils Cyber Command in Response to 'New Era in Warfare'", in *SC Media*, 16 December 2016, https://www.scmagazineuk.com/france-unveils-cyber-command-in-response-to-new-era-in-warfare/article/579671.

[34] See the France's Ministry of Defence website: *Military Planning (2014-19) Act and update (2015-2019)*, 19 July 2017, https://www.defense.gouv.fr/english/dgris/defence-policy/military-planning-2014-19-act-and-update-2015-2019/mp-2014-2019-act-and-update.

[35] France's Ministry of Defence, *Déclaration de M. Jean-Yves Le Drian, ministre de la défense, sur la cyberdéfense*, Bruz, 12 December 2016, http://discours.vie-publique.fr/notices/163003632.html; Valérie Leroux, "Les armées françaises intègrent le combat numérique à leur arsenal", in *AFP*, 12 December 2016, https://fr.news.yahoo.com/armées-françaises-intègrent-combat-numérique-à-arsenal-115324176.html.

[36] Nina Werkhäuser, "German Army Launches New Cyber Command", in *Deutsche Welle*, 1 April 2017, http://p.dw.com/p/2aTfJ.

[37] Justyna Gotkowska, "The Cyber and Information Space: A New Formation in the Bundeswehr", in *OSW Analyses*, 12 April 2017, https://www.osw.waw.pl/en/publikacje/analyses/2017-04-12/cyber-and-information-space-a-new-formation-bundeswehr.

[38] Claudio Graziano, "Cyber Defence. The Joint Cyber Command is Born", Interview with the Chief of Defence Staff in *Informazioni della Difesa*, No. 3/2017, p. 12-15, https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/cyber_defence.pdf.

ISSN 2280-6164

This brief overview demonstrates how countries are structurally addressing cyber threats and enhancing their national capabilities. Many of the countries mentioned above are combining defensive network and critical infrastructure protection policies with the development of offensive measures to counter those risks. International cyber instability is expanding as the cyber threats continue to evolve and countries increasingly respond by developing offensive capabilities. A cyber arms race is well underway.

The United States, China, and Russia have developed and refined their national cyber security strategies over the years, and their capabilities stand out in terms of sophistication. Among the European states, the United Kingdom and France have been the most active in the cyber field, while the rest of the countries have more recently begun to update their policies and national structures.

2. Existing international agreements in other domains

In a new era of networked computing and digital transformation, new technologies bring new economic opportunities but can also introduce new dangers. To reduce the risks of new technological capabilities, the international community has pursued two parallel tracks. On one hand, as rational theorists purport that war and conflict is a part of human nature, we must focus on trying to limit the horrors of war, such as through international binding agreements for legal conduct through the Geneva Conventions. On the other hand, we must seek to limit the proliferation of technologies that could be destructive and destabilizing to the international environment. Previously, this has been done through sanctions or through the adoption of international conventions to ban, or control, the production or exchange of hazardous material and technologies that can be used for malicious purposes. The same reasoning that led to arms control treaties could be applied to cyber weapons.

The first section of this chapter will focus on the expected rules for nation states during wartime, starting from the 1949 Geneva Convention, with the aim of drawing links to the cyber weapons era. The second section will focus on the prohibition or limitation of the proliferation of certain weapons, through a study of the Biological Weapons Convention, the Chemical Weapons Convention and the Non-Proliferation Treaty with the purpose of highlighting the successes and challenges of such treaties. Finally, the last section will analyse the Wassenaar Arrangement. This will help explain one of the main challenges when dealing with cyber offensive capabilities, namely their dual use capacity and the problem of making a clear distinction between offense and defence.

2.1 Regulations on use

Defining appropriate state behaviour during armed conflict – including the justification for engagement a war (*ius ad bellum*) and the acceptable actions in the waging of a war (*ius in bellum*) – dates back many decades. In 1870, Henry

ISSN 2280-6164

Dunant, the founder of the Red Cross, expressed the necessity of declaring certain towns neutral during times of conflict, so that wounded soldiers could be collected or treated without fear of attack. It was the same Dunant that, during the Paris Commune of 1871 tried to set up places which would serve as a refuge for the civilian population. The Hague Conventions, adopted through the diplomatic conferences of 1899 and 1907, were the first attempt by the international community to prescribe nation state norms of conduct during hostilities.

The codification of international humanitarian law (IHL) was further developed through the four Geneva Conventions, agreed to in 1949. The parties to the conventions committed themselves to protect the victims, the civilians not taking active part in the armed conflict, from the consequences of a war. The Geneva Conventions' provisions should be applied in any cases of war or armed conflict arising between two or more parties, even if the state of war is not recognized by one of them, as well as in cases of occupation.[39] To be recognized as "armed conflict"[40] the confrontation must meet certain conditions (a minimum level of intensity and the involvement of minimum organized parties).[41] The Geneva Conventions provide frameworks with four conventions and two additional Protocols (1977) for the conduct during internal or international state conflict.

The fourth convention is the most interesting framework for the purposes of our analysis, due to the protection of civilian populations. This convention provides guidelines for the general protection of civilians in addition to protections to hospitals, neutral zones, to wounded and sick combatants, and to consignments of medical supplies, food, and clothing.[42] The existence of such protection is useful for our analysis since the protection of civilian infrastructure is crucial in the cyber domain. As regards armed conflict in which cyber weapons may be used, the main concern would be the damage that could be inflicted to critical infrastructures. These include power plants, nuclear plants, dams, water treatment and distribution systems, oil refineries, gas and oil pipelines, banking systems, hospital systems, railroads, and air traffic control. In particular, where many of these critical infrastructures rely on supervisory control and data acquisition (or SCADA) systems and distributed control systems (DCS). The potential, massive suffering that could be caused to civilian populations in the context of such attacks is the reason why many academics and researchers have begun to reflect on the need for international frameworks to define acceptable behaviour by a nation state

[39] Geneva Convention (IV) on Civilians, 1949, https://ihl-databases.icrc.org/ihl/INTRO/380.

[40] International Criminal Tribunal for the former Yugoslavia (ICTY), Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction in Case No. IT-94-1, *Prosecutor v. Dućko Tadić*, 2 October 1995, http://www.icty.org/x/cases/tadic/acdec/en/51002.htm.

[41] International Committee of the Red Cross (ICRC), "How is the Term 'Armed Conflict' Defined in International Humanitarian Law?", in *ICRC Opinion Papers*, 17 March 2008, https://www.icrc.org/eng/resources/documents/article/other/armed-conflict-article-170308.htm.

[42] Jean S. Pictet (ed.), *Commentary on the Geneva Conventions of 12 August 1949, Vol. 4: Geneva Convention relative to the Protection of Civilian Persons in Time of War*, Geneva, ICRC, 1958, https://www.loc.gov/rr/frd/Military_Law/pdf/GC_1949-IV.pdf.

DOCUMENTI IAI 18 | 03 - MARCH 2018 ISSN 2280-6164

during cyber operations.

The concept of "attack" is at the core of IHL, and the basis for several limitations and prohibitions in armed conflicts: "attacks" means "acts of violence against the adversary, whether in offence or in defence".[43] The use of violence against a target is what distinguishes an attack from other military operations. Therefore, non-violent operations such as cyber espionage could not be placed in this category. However, it is widely accepted that such definitions do not refer solely to how this attack is carried out, but also to the violence of its consequences.[44] Accordingly, if a cyber operation alters the SCADA system controlling air traffic, causing any sort of physical destruction, this would undoubtedly be considered as an attack.

The most relevant aspects of IHL are the principles of distinction, proportionality and precaution. According to the principle of distinction,

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[45]

In other words, the only attacks which are permitted under the provisions of IHL are the ones targeting military objects; any operations targeting civilian objects will be declared unlawful. Accordingly, a cyber-attack should be directed solely against appropriate legal targets, such as military installations. In cyber space, because of the deep interconnectedness of civilian and military infrastructure, it is difficult to differentiate between military and civilian objectives. Because of such interconnectedness and ambiguity in the digital world, one challenge is when an attack is specifically targeted at a lawful target, such as a military object, there could easily be unintended consequences that could cause damage to civil infrastructure as well.[46] Another major problem relates to dual-use material. In fact, some of the digital infrastructure upon which our society relies, could be considered a dual-use material and therefore, a legitimate military target.[47] Today, there are no satisfactory solutions to this problem within the framework of IHL. Further development and clarification to existing legal frameworks is necessary to overcome this *impasse*,

[43] See ICRC website: *Rule 1. The Principle of Distinction between Civilians and Combatants*, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter1_rule1.

[44] Michael N. Schmitt (ed.), *Tallinn Manual 2.0*, cit., p. 415-417.

[45] Art. 48 of the Additional Protocol (I) to the Geneva Conventions, 1977, https://ihl-databases.icrc.org/ihl/INTRO/470.

[46] Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians", in *International Review of the Red Cross*, Vol. 94, No. 886 (Summer 2012), p. 533-578, https://www.icrc.org/eng/assets/files/review/2012/irrc-886-droege.pdf.

[47] Robin Geiß and Henning Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space", in *Israel Law Review*, Vol. 45, No. 3 (November 2012), p. 381-399, https://core.ac.uk/download/pdf/16457774.pdf.

© 2018 IAI
ISSN 2280-6164
DOCUMENTI IAI 18 | 03 - MARCH 2018

and to guarantee protection to civilians and civilian infrastructure.

Despite the above-mentioned difficulties in the application of IHL to cyber operations, some specific provisions could be implemented in cyber space. IHL prohibits indiscriminate attacks, as well as indiscriminate means and methods of warfare, thus, it constrains the use of any kind of weapon which are unable to distinguish between military and civilian targets.[48] In cyber space, such a principle would mean that, for instance, a virus or piece of malware which is designed to attack a specific military target only, could be classified as lawful under international humanitarian law. Following the same principle, nation states should not use a virus which replicates without any possibility of being controlled.[49]

The principle of proportionality concerns the protection of civilian populations through the prohibition of indiscriminate attacks. Specifically, attacks are viewed as indiscriminate if they are "expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated".[50]

The applicability of this principle to cyber operations finds its justification in the idea that nowadays it appears counter-intuitive and outdated for only the physical destruction of objects to be included in the interpretation of the proportionality principle.[51] Thus, also the loss of functionality, even in the absence of physical damage, could be considered as a relevant factor in the evaluation of the proportionality of an attack. Applying the interpretation of this principle to cyber space leads to significant questions about how to interpret proportionality and the measure for corresponding damages.[52]

Even though the principle of proportionality can be applied to cyber operations, some limitations must be considered, due to the indirect or unintended consequences and collateral damage.[53] This implies that when a cyber-attack is carried out, the decision-maker should carefully take into consideration not only the direct effects, but also potential collateral damage.[54] Clearly, in cyber space the ability to predict the outcome of an attack is increasingly difficult compared to traditional kinetic

[48] International Court of Justice (ICJ), *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*, 8 July 1996, http://www.icj-cij.org/en/case/95/advisory-opinions.

[49] Art. 51 of the Additional Protocol (I) to the Geneva Conventions, cit.

[50] Ibid.

[51] Robin Geiß and Henning Lahmann, "Cyber Warfare",cit.

[52] Eric Boylan, "Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners", in *Vanderbilt Journal of Transnational Law*, Vol. 50, No. 1 (February 2017), p. 217-244, https://www.vanderbilt.edu/jotl/2017/02/applying-the-law-of-proportionality-to-cyber-conflict-suggestions-for-practitioners.

[53] Ibid.

[54] Eric Talbot Jensen, "Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations", in *American University International Law Review*, Vol. 18, No. 5 (2003), p. 1145-1188, http://digitalcommons.wcl.american.edu/auilr/vol18/iss5/3.

ISSN 2280-6164

operations, mainly due to the above-mentioned interconnectedness and speed of the cyber world.

Finally, the third basic principle of IHL is the principle of precaution. Such a principle must be applied both when the state is the aggressor, and when it is the victim. The first aspect of the principle is referred to precautions in attacks, and it mandates that nation states carrying out an attack should apply whatever means to spare civilian lives and objects. Specifically, the article requires steps to verify that targets are military objects.[55] On the other hand, it requires that the parties to conflicts "to the maximum extent feasible [...] endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives" and "take the other necessary precautions to protect the civilian population".[56]

Fulfilling this principle in the cyber domain, according to the Tallinn Manual, would require the separation of civil and military cyber infrastructure. However, this measure is particularly difficult to apply in cyber space because of the dual-use nature of some technologies, as described above.

Due to the continued ambiguity in the application of international humanitarian law to cyber space, it is clear that further dialogue is needed to address these gaps, and how we can build new agreements.[57]

2.2 The regulation of proliferation

Usually, non-proliferation agreements appear as contractual undertakings adopted because of a common political interest. According to several academic researchers, arms control treaties are often the product of a policy choice rather than a legal necessity.[58] The purpose of non-proliferation regimes includes: minimizing instability; increasing predictability in relations between potentially hostile states; pre-empting the development of new weapons; contributing to conflict management by establishing a framework to enable negotiations among parties, generally fostering a non-hostile atmosphere. The main reason for this international settlement was that those weapons were recognized as able to cause unprecedented levels of destruction, thus their proliferation would have harmed

[55] Art. 57 of the Additional Protocol (I) to the Geneva Conventions, cit.

[56] Art. 58 of the Additional Protocol (I) to the Geneva Conventions, cit.

[57] Eric Talbot Jensen, "Cyber Attacks: Proportionality and Precautions in Attack", in *Naval War College International Law Studies*, Vol. 89 (2013), p. 198-217, http://digital-commons.usnwc.edu/ils/vol89/iss1/15.

[58] For more on the topic see, for example: Richard K. Betts, "Systems for Peace or Causes of War? Collective Security, Arms Control, and the New Europe", in *International Security*, Vol. 17, No. 1 (Summer 1992), p. 5-43; David Davenport, "The New Diplomacy", in *Policy Review*, No. 116 (December 2002/January 2003), p. 17-30, https://www.heritage.org/node/18600; and Andrew P. Cortell and James W. Davis, "How Do International Institutions Matter? The Domestic Impact of International Rules and Norms", in *International Studies Quarterly*, Vol. 40, No. 4 (December 1996), p. 451-478.

ISSN 2280-6164

the international community. The main characteristics of such weapons of mass destruction (WMD) are large-scale destruction and indiscriminate nature of the effect, notably against civilians.

The three treaties regulating WMDs are the Non-Proliferation Treaty (NPT), the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC). We will analyse these treaties in order to draw lessons that can be used to stop the proliferation of cyber weapons.

The NPT was the first international arms control regime to be signed to limit the proliferation of nuclear weapons.[59] By the end of the Cold War, many countries had nuclear ambitions. The treaty established a differentiated treatment for nuclear-weapons states – consisting of the United States, Russia, China, France, and the United Kingdom – and non-nuclear-weapon states.[60] The International Atomic Energy Agency (IAEA) was in charge of both promotion of peaceful development of civil nuclear power and control over the diffusion of offensive nuclear capabilities. The IAEA has a central role in the process of implementation of the treaty. It assists non-nuclear-weapon states which lack the necessary knowledge and expertise in using nuclear technology for peaceful purposes and verifies that treaty participants are honouring their international legal obligations not to develop nuclear weapons for offensive purposes. Despite its near-universal membership and the IAEA's assistance in enforcement and transparency, the NPT is still facing obstacles. The primary obstacle is the lack of progress towards nuclear disarmament by the five NPT-nuclear-weapons states, and the stalemate in obtaining a WMD-free zone in the Middle East region.

The second international proliferation treaty we will analyse is the BWC, entered into force in 1975. The destructive potential of biological weapons persuaded the international community on the need for limitations for the use of biological weapons. The BWC prohibits the development, production, acquisition, transfer, stockpiling and use of biological and toxin weapons. By 2017, it was signed by almost all countries, with only eleven states having not signed or ratified.[61] Notably, the BWC was the first multilateral disarmament treaty banning an entire category of weapons of mass destruction. Under the provision of the BWC, signatory nation states renounce their right to engage in military preparation of biological warfare. To effectively implement the Convention's guidelines, State parties are required to translate their commitments into adequate national actions.

However, negotiations to establish mechanisms to verify signatory nation-state compliance with the ban have been unsuccessful. The current ban does not

[59] Opened for signature in 1968, the treaty entered into force in 1970.

[60] As for 2017, 191 states have signed the treaty, although North Korea withdrew from it in 2003. Four UN member states (India, Israel, Pakistan and South Sudan) have not ratified nor signed the treaty. Notably, the first three are thought to possess nuclear weapons.

[61] Chad, Comoros, Djibouti, Eritrea, Israel, Kiribati, Micronesia, Namibia, Niue, South Sudan and Tuvalu.

ISSN 2280-6164

include any enforcement mechanism: neither international inspectors nor rules governing research and development of possible bioweapons. A major effort to overcome this impasse was discussed during the 2006 Sixth Review Conference. The conference succeeded in comprehensively reviewing the Convention and the signatory nation-states agreed on important steps, such as increasing their effort to promoting universal adherence to the convention, updating and streamlining the procedures for submission and distribution of confidence building measures (CBMs), support comprehensive intersessional programmes, and establish an Implementation Support Unit (ISU) to assist State parties to enforce the Convention.[62] Accordingly, a few initiatives are currently underway to strengthen the international observance of the treaty. Many countries have, for example, adopted national legislation to criminalize bioweapons research activities.

Lastly, the CWC, which entered into force in 1997, prohibits the development, production, stockpiling, acquisition or transfer of chemical weapons.[63] It is the first disarmament agreement negotiated within a multilateral framework that compels signatory states to eliminate an entire category of WMD under international supervision. In fact, the treaty works under the umbrella of the Organization for the Prohibition of Chemical Weapons (OPCW), an intergovernmental body tasked with overseeing the verification of the treaty's provisions. The treaty has banned the use of chemical weapons but also commits nations to eliminating existing stockpiles. It is the most successful example of an arms control treaty – in terms of adherence, enforcement and verification – to date. As of 2017, 192 states have ratified the treaty. A key component for the success of OPCW has been the active participation of the global chemical industry.[64]

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is additional an international framework which seeks to establish limitations on the proliferation of military technologies. The Wassenaar Arrangement (WA) established an export control regime for all items included in lists for dual-use goods, technology, and munitions.[65] It complements and reinforces the control regimes of WMDs. Measures are implemented on the basis of national discretion, and no formal mechanism to enhance the arrangement is provided.

This survey of non-proliferation treaties and initiatives enable us to draw several conclusions. First, each of the three arms control conventions resulted from the

[62] See the UN Office for Disarmament Affairs (UNODA) website: *Biological Weapons*, https://www.un.org/disarmament/wmd/bio.

[63] Organization for the Prohibition of Chemical Weapons (OPCW), *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction* (Chemical Weapons Convention), 13 January 1993, https://www.opcw.org/chemical-weapons-convention.

[64] Laura Reed, *Weapons of Mass Destruction*, Hampshire College Peace and World Security Studies: Conflict Topics, https://www.hampshire.edu/node/35664.

[65] See the Waassenaar Arrangement website: *Control Lists*, http://www.wassenaar.org/?p=17.

DOCUMENTI IAI 18 | 03 - MARCH 2018
ISSN 2280-6164

awareness of the devastation and the destructive potential caused by weapons of mass destruction, compelling the need to take measures to safeguard civilian populations. Considering this, all conventions have succeeded in achieving global reach. Second, two of the three treaties established agencies devoted to verifying treaty compliance. These arms control regimes set up to safeguard civilians and increase international stability provide insights to take into consideration for a potential proliferation regime for cyber weapons.

Supporting the idea of cyber weapons as weapons of mass destruction, the Hoover Institution coined the term "electronic weapons of mass destruction" (eWMD). Of increasing concern is the potential consequences of a cyber-attack targeting SCADA systems. In our modern, digital economy, considering the dependence of our society on critical infrastructure, eWMD have the potential to be the cyber equivalent of a military blockade.[66] Similarly, as underlined by Clay Wilson, the acronym "CBRNCy" (chemical, biological, radiological, nuclear, and cyber) is now used by the International Working Group, Landau Network Centro Volta, to include new cyber threats as part of their ongoing discussions on WMD and non-proliferation.[67]

There is no shortage of academic researchers who provide further analysis and conclusions on the issue. According to Jeffrey Carr, a cyber weapons cannot be classified as a weapon of mass destruction because so far they are not able to kill or injure humans as efficiently as guns or bombs, and no historical or legal evidence is in support of such classification.[68] Under the definition of the US Code, no use of cyber weapons qualifies as use of a weapon of mass destruction, in the legal, historical, or vernacular senses of the term.[69] The same position emerged from the interviews conducted during our research activities. Many academic researchers agreed with the idea that not having yet caused any casualties, it is particularly difficult to categorize cyber weapons as weapons of mass destruction.

However, the debate over the definition of cyber weapons as weapons of mass destruction is not the threshold which needs to be considered in the evaluation of the feasibility of a control regime for cyber space. Significant political attention is currently paid to the issue, fuelled by the WannaCry and NotPetya attacks. Cyber

[66] John J. Kelly and Lauri Almann, "eWMDs", in *Policy Review*, No. 152 (December 2008/January 2009), p. 39-50, http://www.modelsoftware.com/people/152KellyAlmannOffprint.pdf.

[67] Clay Wilson, "Cybersecurity and Cyber Weapons: Is Nonproliferation Possible?", in Maurizio Martellini (ed.), *Cyber Security. Deterrence and IT Protection for Critical Infrastructures*, Cham, Springer, 2013, p. 17.

[68] Jeffrey Carr, "The Misunderstood Acronym: Why Cyber Weapons aren't WMD", in *Bulletin of the Atomic Scientists*, Vol. 69, No. 5 (2013), p. 32-37.

[69] Ibid. According to the US Code Title 18, Section 2332a, a weapon of mass destruction is "any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; any weapon involving a biological agent, toxin, or vector; any weapon that is designed to release radiation or radioactivity at a level dangerous to human life". See US Code Section 2332a: *Use of weapons of mass destruction*, https://www.law.cornell.edu/uscode/text/18/2332a.

© 2018 IAI ISSN 2280-6164 DOCUMENTI IAI 18 | 03 - MARCH 2018

threats are increasingly seen with great concern all over the world, and nation states are taking concrete actions to deal with them. Cyber offensive capabilities could potentially have considerable destructive power and could kill large amounts of people if deployed against certain targets. In this respect for example, many academic researchers are investigating how a cyber-attack could target a nuclear facility,[70] and other critical infrastructure. This results from the dual-use of cyber offensive capabilities and the need to take this aspect into account in the process of building a proliferation regime in cyber space. Two characteristics of the cyber domain do create unique challenges for any arms control regime. Primarily, cyber-attacks can be carried out in relative anonymity. The peculiarity of secrecy and plausible deniability of the attack makes it very hard to sanction the states from which the attack has been carried out. Therefore, any constraint in the use of cyber weapons would at least require a solution to the "attribution" problem. Moreover, malicious software is abundant and extremely difficult to identify and suppress. Therefore, an international agreement on cyber arms control would currently face serious problems with verification and enforcement. These aspects will be better evaluated in the fourth chapter.

3. Analysis of multilateral initiatives in the cyber domain

Multilateral cyber diplomacy has led to different ways of addressing the issue. Several studies have been conducted to determine how and if international law applies to cyber space and whether new legal frameworks are needed. In 1998, the Russian Federation submitted a draft proposal to the First Committee of the UN General Assembly on the "Developments in the field of information and telecommunications in the context of international security".[71] That resolution was adopted by the General Assembly, and since then, has been updated through resolutions calling for the different views of UN member states on the issue of information security.

Cyber threats and expected state behaviour in cyber space have also been addressed by the UN Group of Governmental Experts (UNGGE), established in 2004. At the time, the first 15-member UNGGE did not reach a consensus report mainly because of two policy issues: (a) the definition of a threshold for threats posed by nation state exploitation of ICTs and (b) whether the focus should be on information

[70] On the matter, please refer to: Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack", in *Strategic Insights*, Vol. 10, No. 1 (Spring 2011), p. 15-25, http://www.dtic.mil/dtic/tr/fulltext/u2/a541955.pdf; James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", in *Survival*, Vol. 53, No. 1 (2011), p. 23-40; Oona A. Hathaway et al., "The Law of Cyber-Attack", in *California Law Review*, Vol. 100, No. 4 (August 2012), p. 817-885, http://www.californialawreview.org/?p=2129.

[71] See the UN Office for Disarmament Affairs (UNODA) website: *Developments in the field of information and telecommunications in the context of international security*, https://www.un.org/disarmament/topics/informationsecurity.

ISSN 2280-6164

content or on information infrastructure.[72] The group adopted next steps focused on: (a) protection of critical infrastructure; (b) confidence-building measures; (c) information exchange on national legislations, policies and technologies; (d) elaboration of common terms and definitions on information security.[73] Although the group reached a consensus report in 2013, no practical implementation mechanisms were included.

In 2015, UNGGE achieved a landmark consensus report.[74] The report identified a number of cyber "norms" or expected state behaviour in cyber space. During the G20 Antalya Summit, the 2015 UNGGE report was referenced in the Leader's Communiqué, which represented a successful step forward in including a wider group of countries, some of whom were not participants in UNGGE process.[75]

Unfortunately, the 2016/2017 UNGGE was not able to come to a consensus report particularly with respect to the applicability of international law in cyber space. Because of this impasse, the group was unable to produce a final consensus report.[76] Two official documents express this lack of consensus, both dated 23 June 2017: the declaration by the representative of the United States, Michele Markoff, and by the representative of Cuba, Miguel Rodrìguez. The main area of contention was around the applicability of international law for cyber space. These questions revolved around the difficulties in defining the threshold for armed conflict in cyber space and the subsequent right to self-defence.

A stalemate emerged between three countries – China, Russia, and Cuba – and the western "like-minded" countries, primarily led by the United States. Cuba, Russia and China did not accept any threshold that would trigger the right to self-defence, and strongly denounced the "equivalence between the malicious use of ICTs and the concept of 'armed attack'".[77] The United States and its allies in the "like-minded group" instead stressed the necessity of discussing a peaceful dispute resolution for conflict in cyber space, but also considered nation state response to

[72] UN Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/60/202), 5 August 2005, http://undocs.org/A/60/202.

[73] UN Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/65/201), 30 July 2010, http://undocs.org/A/65/201.

[74] UN Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174), 22 July 2015, http://undocs.org/A/70/174.

[75] G20 Leaders' Communiqué, Antalya, 16 November 2015, http://www.g20.utoronto.ca/2015/151116-communique.html.

[76] Elaine Korzak, "UN GGE on Cybersecurity: The End of an Era?", in *The Diplomat*, 31 July 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe.

[77] Miguel Rodrìguez, *Declaration by the Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 23 June 2017, https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf.

DOCUMENTI IAI 18 | 03 - MARCH 2018
ISSN 2280-6164

malicious cyber activity as lawful under existing international law.[78] Although the 2017 UNGGE was also unable to come to a final consensus report, the previous consensus reports remain.

While the UNGGE discussions focused on the development of norms, Russia and China have continued to push for a treaty or convention for cyber space. In 2011, Russia and China, supported by the Shanghai Cooperation Organization (SCO), proposed an International Code of Conduct for Information Security.[79] The draft consisted of a voluntary-based code of conduct, open to all UN member states Among other things, the draft called for UN member states to: (a) comply with the Charter of the UN also with respect to information technologies; (b) not to proliferate information weapons; (c) bolster bilateral, regional and international cooperation; and (d) settle disputes without the use of force. In January 2015, SCO states tried again to propose their view on regulating information security within the UN Assembly, with the objective to "push forward the international debate on international norms on information security, and help forge an early consensus on this issue".[80] This version underscored the idea that sovereignty and territoriality in the digital space should be internationally recognized. The western "like-minded" group viewed this development to be potentially at odds with an open, secure and stable Internet, as they viewed Russia's ultimate ambition to use such a mechanism to control content and speech online.

In the 2011 draft convention, Russia broadly define the term "information security" as "a state in which personal interests, society, and the government are protected against the threat of destructive actions and other negative actions in the information space".[81] The term, defined as such, may be controversial. In fact, if on the one hand it includes measures to counteract malicious acts online, on the other hand, it may serve as a basis to control the spread of information itself, with strong implications for the censorship of content that states do not consider appropriate.

Apart from content control, a second source of concern refers to Internet governance. The document notes that "States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security,

[78] Michele G. Markoff, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, Remarks by the US Department of State Deputy Coordinator for Cyber Issues*, New York, 23 June 2017, https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm.

[79] UN General Assembly, Letter dated 12 September 2011..., cit.

[80] UN General Assembly, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* (A/69/723), 13 January 2015, http://undocs.org/A/69/723.

[81] Russia's Ministry of Foreign Affairs, *Convention on International Information Security*, cit. See also Keir Giles, "Russia's Public Stance on Cyberspace Issues", cit.

ISSN 2280-6164

continuity and stability of operation, and its development [...]".[82] Such a principle could be summarized with "Internet policy authority". In this respect, the risk of an exclusively state-determined arena may be present.

The concept of content control compounded with nation state dominance of the cyber domain can lead to pervasive information control of any contents deemed politically sensitive by governments with consequent threat to freedom of speech. Finally, it should be noted that the code of conduct proposed by the SCO states lacks data protection and personal privacy related provisions.

NATO has also tackled the issue on both a strategic and operational domain. On the strategic side, NATO has developed a Cyber Defence Strategy, adopted since the Wales Summit of 2014 and strengthened by the Cyber Defence Pledge at the Warsaw Summit of 2016.[83] The Pledge reaffirms the applicability of international law in cyber space, supports the adoption of voluntary norms of responsible state behaviour, and establishes cyber confidence-building measures. The recognizable contribution of NATO creating an *opinio iuris* regarding the applicability of existing international agreements is valuable in furthering multilateral initiative in the cyber domain. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Tallinn, Estonia has also made significant contributions to the cyber norms discussion through the publication of the Tallinn Manual in 2013.[84] Last year, NATO CCDCOE updated the manual and released the Tallinn Manual 2.0.[85] The Tallinn manuals provide significant contributions to the legal analysis of how international law applies in cyber space. However, it is only a legal analysis and does not bind governments to its findings.

The themes shift from the prohibition of the use of force in cyber operations, to the right to exercise self-defence, to cyber incidents which fall below the threshold of the use of force or armed conflict.

It is important to note that lawyers drafting the Tallinn Manual were unable to reach a consensus on several components of how international law applies in cyber space.[86]

NATO's strategic approach also includes cooperation with the EU. The implementation roadmap has seen a first crucial step in the adoption of the Technical

[82] UN General Assembly, *Letter dated 9 January 2015*..., cit., p. 5.

[83] NATO, *Cyber Defence Pledge*, 8 July 2016, https://www.nato.int/cps/su/natohq/official_texts_133177.htm.

[84] Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013.

[85] Michael N. Schmitt (ed.), *Tallinn Manual 2.0*, cit.

[86] Kalev Letaruu, "What Tallinn Manual 2.0 Teaches Us about the New Cyber Order", in *Forbes*, 9 February 2017, https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order.

ISSN 2280-6164

Arrangement on Cyber Defence signed on 10 February 2016.[87] This document allows both organizations to exchange cyber-defence related information through the NATO Computer Incident Response Capability (NCIRC) and the EU Computer Emergency Response Team (CERT-EU). This agreement is one of the major examples regarding how to facilitate technical information sharing among nation states to improve incident prevention, detection, and response.

Cyber space is largely produced, operated, and managed by the private sector. As the tech sector plays a unique role as the Internet's first responders to threats, it is important that any agreement for cyber space include the private sector. The ICT industry serves as both the frontline and first responders during cyber-attacks and for this reason, in efforts to improve cyber security, the need for a multi-stakeholder approach is an operational reality rather than an ideology.

Nevertheless, the international community still fails to capture the key role of the private sector in providing security in cyber space. There is only a limited number of platforms for discussion and policy-development that incorporate all the major stakeholders, including the private sector. NATO has recognized this issue to involve the private sector as a key player in cyber space and started the NATO Industry Cyber Partnership (NICP). The NICP is a partnership which comprises NATO countries' industry representatives, national CERTs, and NATO entities. In this organization information-sharing activities, multinational Smart Defence projects and other forms of cooperation are developed.[88] NATO is therefore one of the most active international organizations facing the issue of threats in cyber space. Although due to the nature of NATO, it sponsors a defensive technical approach, its efforts to apply international law to cyber issues is a milestone for consensus building within the international arena.

Another organization which is contributing to consensus building through common actions by member states is the European Union through the European Commission and the European External Action Service (EEAS). The Commission clearly expressed its key objectives in the field of cyber security: (a) increase cyber security capabilities and cooperation; (b) make the EU a strong player in cyber security; and (c) mainstream cyber security in EU policies. The EU started to face the issue from a security point of view, keeping the focus on cybercrime.

Regulatory measures have been adopted by the Commission to improve the overall level of cyber security in the EU. The strength of the Directive on Security of Network and Information Systems lies in the minimum security requirements for EU member states in order to improve cyber security risk management.[89] The

[87] EEAS, *EU and NATO Increase Information Sharing on Cyber Incidents*, 10 February 2017, http://europa.eu/!QM73By; NATO, *NATO and the European Union Enhance Cyber Defence Cooperation*, 10 February 2017, https://www.nato.int/cps/en/natohq/news_127836.htm.

[88] See the NCIP official website: http://www.nicp.nato.int.

[89] The so-called NIS Directive entered into force in August 2016. See Directive (EU) 2016/1148

ISSN 2280-6164

directive requires member states to implement a Computer Security Incident Response Team (CSIRT) and a competent national authority, then cooperation will be assured through the CSIRTs network. The directive also applies to the private sector to protect civilian infrastructure of digital service providers. This legislative instrument underlines the efforts to cooperate with the private sector and the necessity of information sharing to better tackle issues related to cyber security.

The EU has recognized the need for greater capacity to support the implementation of the NIS Directive and facilitate international cooperation to reinforce the EU's resilience and deterrence to external attacks. The European Agency for Network and Information Security (ENISA) performs this role and develops cyber security guidance and capacity building expertise for EU member states.[90]

Alongside the NATO CCDCOE, the EU is also working on cyber defence initiatives and international cooperation. In October 2016, the Council of the EU established a Horizontal Working Party on Cyber Issues to ensure strategic coordination of cyber issues amongst EU member states. The Working Party advises on EU priorities and strategic objectives in the policy area of cyber space and supports effective external representation of the EU.[91]

On 7 June 2017, the first outcome of the Working Party was adopted: the Council agreed to develop a framework for a Joint EU diplomatic response to malicious cyber activities, the so-called "Cyber Diplomacy Toolbox", that is undergoing further revision and is not yet publicly available.[92] It is however clear that international collaboration amongst EU member states is based on the idea of using diplomatic measures within the EU to counteract cyber threats.

Although, the Cyber Diplomacy Toolbox does not specify the specific, diplomatic tools themselves, the circumstances when they may be used and related threshold of the "use of force" or "armed conflict", the Toolbox leaves attribution open to the selection of appropriate and proportionate measures without deepening the analysis of cyber operations.[93] Development of the Toolbox demonstrates the

concerning measures for a high common level of security of network and information systems across the Union, 6 July 2016, http://data.europa.eu/eli/dir/2016/1148/oj.

[90] See European Commission, *Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")* (COM/2017/477/3), 22 February 2018, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52017PC0477R(02).

[91] Council of the European Union, *Horizontal Working Group on Cyber Issues - Establishment and adoption of its Terms of Reference* (13114/16), 20 October 2016, http://data.consilium.europa.eu/doc/document/ST-13114-2016-INIT/en/pdf.

[92] Council of the European Union, *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* (9916/17), 7 June 2017, http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

[93] Katriina Härmä and Tomáš Minárik, "European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox", in *Incyder News*, 18 September 2017, https://ccdcoe.org/node/1221.html.

ISSN 2280-6164

search for a common position on international cyber threats, thus placing the Toolbox among powerful instruments to address the issue.

Furthermore, the reader's attention must be drawn to the Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises, annexed to the Commission Recommendation of the 13 of September 2017.[94] This Blueprint presents a strategic, political, operational and technical response to cyber-attacks at the European-level. The guiding principles set by the Blueprint are proportionality, subsidiarity, complementarity and confidentiality of information. Subsequently, the core objectives are effective response, shared situational awareness and public communication messages. Although these set of measures show a great commitment of member states in terms of cyber security at the European-level, the Commission and EEAS do not equally reflect this outside the EU for a stronger binding legal instrument to face cyber threats. Despite this relatively strong framework for cyber security to protect citizens and visitors in the EU, the interdependent nature of the cyber domain demands further effort by the EU to achieve similar protection globally. However, it is unlikely that the EU would encourage any international agreement in future at the UN-level so the EU will continue towards deterrence via diplomatic toolboxes.

Recognizing that international agreements may take a decade or longer to achieve, it is important to pair long-term aspirations with immediate short-term steps to improve cyber security and prevent conflict in cyber space. Focusing on the creation of cyber confidence building measures (CCBMs) is an important component in increasing trust through voluntary sharing of information and transparency between states and other stakeholders. Since 2013, the Organization for Security and Co-operation in Europe (OSCE) have developed CCBMs "to reduce the risks of conflict stemming from the use of information and communication technologies".[95]

OSCE's plan is implemented in three stages: (a) adoption of transparency measures; (b) development of cooperation measures; and (c) adoption of stability measures. Transparency target the sharing of national approaches towards national cyber strategies and CCBMs. Cooperation focuses on mutual assistance for capacity-building initiatives, such as the establishment of CERTs or cooperation in drafting legislation. Stability aims to strengthen nation states' commitment to refrain from certain types of destabilizing activities.[96]

[94] European Commission, *Commission Recommendation (EU) 2017/1584 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises* (C/2017/6100), 13 September 2017, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32017H1584.

[95] Organization for Security and Co-operation in Europe (OSCE), *Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies* (PC.DEC/1106), 3 December 2013, http://www.osce.org/pc/109168.

[96] Patryk Pawlak, "Confidence-Building Measures in Cyberspace: Current Debates and Trends", in Anna-Maria Osula and Henry Rõigas (eds.), *International Cyber Norms. Legal, Policy & Industry*

ISSN 2280-6164

The OSCE's Decision No. 1202 represents a significant achievement in adoption of comprehensive CBMs.[97] In addition to the OSCE, several other regional fora such as the Association for South East Asian Nations (ASEAN) and the Organization of American States (OAS) are also developing CBMs.[98] Although these initiatives had not evolved since their launches, they still confirm a global interest in securing cyber space[99] and ASEAN published a paper on cyber norms in 2017.

In order to be as comprehensive as possible, this study must include regimes on export control. The first global multilateral arrangement on export controls for conventional weapons and sensitive dual-use goods and technologies, so-called Wassenaar Arrangement (WA), expanded its list of dual-use material in 2013 to include "intrusion software". The terms used within the negotiations have raised concerns among stakeholders and practitioners in the field. In fact, stakeholders from the private sector believe the agreement is counterproductive and instead should focus on the importance of sharing exploitations of software to mitigate security vulnerabilities. Dual-use regulation is also under discussion within the EU, which regulates its export through EC regulation No. 428/2009.[100] As for the WA, the regulation raised concerns among practitioners. They are indeed worried that a new update may contain overly generic provisions and may stop research and cooperation. The lack of experts from the private sector and security researcher community at the negotiation tables has led to a significant lack of expertise which has hindered the implementation of an effective export control regime.[101]

Perspectives, Tallinn, NATO CCDCOE, 2016, p. 129-153, https://ccdcoe.org/node/956.html.

[97] Organization for Security and Co-operation in Europe (OSCE), *Decision No. 1202: OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies* (PC.DEC/1202), 10 March 2016, https://www.osce.org/pc/227281. See also Stephanie Liechtenstein, "The OSCE's Pioneering Work on Cyber Security", in *Security and Human Rights Monitor*, 4 April 2016, https://www.shrmonitor.org/osces-pioneering-work-cyber-security.

[98] ASEAN Regional Forum, *ARF Work Plan on Security of and in the Use of Information and Communications Technologies*, 7 May 2017, http://aseanregionalforum.asean.org/events/3-content/public-library/665-plan-of-action-and-work-plans.html; OSA, *Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity* (AG/RES. 2004 (XXXIV-O/04)), 8 June 2004, http://www.oas.org/xxxivga/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm.

[99] Patryk Pawlak, "Confidence-Building Measures in Cyberspace: Current Debates and Trends", cit.

[100] Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, 5 May 2009, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32009R0428.

[101] Markus Maybaum and Jens Tölle, "Arms Control in Cyberspace – Architecture for a Trust-Based Implementation Framework Based on Conventional Arms Control Methods", in Nikolaos Pissanidis, Henry Rõigas and Matthijs Veenendaal (eds.), *8th International Conference on Cyber Conflict. Proceedings 2016*, Tallinn, NATO CCDCOE, 2016, p. 159-173, https://ccdcoe.org/node/1039.html.

ISSN 2280-6164

4. Future perspectives for a cyber convention

The previous chapters allowed us to identify key topics of interest such as: attribution, verification, enforcement, threshold for recognizing a cyber-attack as a "use of force" or "armed conflict", active defence, the indirect or unintended consequences and collateral damage, dual-use and segregation of civilian and military infrastructures, sovereignty, right of self-defence, role of experts of the private sectors and of CERTs, confidence building measures, information sharing, and proxy states. The scope of this section is to highlight these topics in the context of international law, the Geneva Conventions, analogue arms control treaties and international cyber initiatives.

First, we will highlight some terminology issues. As described throughout this study, there is a lack of consensus around various terms, such as cyber space, cyber-attack, etc. The western like-minded group tends to view cyber space as physical and non-physical components which store and exchange data using computer networks; the protection of cyber space refers to both the Internet and infrastructure which makes the exchange of information possible. Following this definition, pieces of hardware are part of cyber space and should be protected. The scope of this definition acknowledges the physical nature of cyber space, which is therefore not indefinite, even though some doctrine criticizes the need for an agreement on the control of cyber weapons on the basis that cyber space is indefinite.

The duality between information warfare and cyber warfare has been addressed by many studies. The EastWest Institute recognizes the duality of the term and first worked on linguistic solutions to deal with its content.[102] A similar initiative – including US, Russia, China, Israel, Iran and several European countries, in which those nation states could agree upon a common vocabulary for cyber terminology – would be a crucial step.

Information warfare terminology has a broader spectrum than cyber warfare and, as examined in the third chapter, raises concerns about content control. The already observed proposal advanced by the Russian government in 2011 within the UN with the support of SCO states, would pave the way for more control on content. In practical terms, the idea of contrasting information warfare would widen the scope also to include the substance of content and not only its form. Information warfare and cyber warfare cannot be considered synonyms and should be treated separately in future negotiations. Intrusions within democratic processes and institutions, through propaganda or through sponsored content on social media may not be considered an act of war, or as a cyber-attack.

[102] James B. Godwin et al. (eds.), "The Russia-U.S. Bilateral on Cybersecurity. Critical Terminology Foundations 2", in *EastWest Institute Policy Reports*, No. 2/2014 (March 2014), https://www.files.ethz.ch/isn/178418/terminology2.pdf.

ISSN 2280-6164

While a consensus around the term will be pursued, the adoption of "information warfare" as a taxonomy could be misleading. "Information warfare" also connects to the idea of Internet governance and sovereignty. Both the 2015 UNGGE report and the SCO 2015 code of conduct proposal underline the idea that sovereignty and territoriality in the digital space should be recognized.[103] Recognition of sovereignty could mean acceptance of state control of cyber space accompanied by the risks for freedom of expression and spreading of authoritarianism in cyber space. The wrong outcome may be realized if an international discussion on this issue does not take place at a global level including the private sector.

A common agreement regarding Internet governance is a vital condition for the future of communications, negotiations, but also the daily life of every citizen. The matter of internet authority governance is a key topic, also in correlation with IP address allocation and the Internet Assigned Numbers Authority (IANA) that is being restructured. IP addresses should be included in the discussion for future regulation towards an international agreement on cyber issues. Unsurprisingly, the increasing risk posed by the spreading of new technology is outlined by many experts, such as the Carrier Grade Network Address Translation (CGNAT), particularly in Europe by Europol and the Estonian Presidency of the EU.[104]

The issue is also related to the transition to the IPv6 protocol, which would mean more secure networks. Although new technologies such as IPv6 and DNSsec may drive the Internet on a more secure and stable path, this can only be successfully achieved together with a stronger commitment from nation states and a common approach towards a vision of the web as a generator of global progress.

To reach a common agreement between nation states, trust is essential. This also applies to cyber discussions since many actors are trying to foster cooperation through CBMs, from NATO and the EU to the OSCE. The fact that a defensive structure such as NATO, has adopted the Cyber Defence Pledge to establish CBMs underlines the importance of such a measure in building trust among NATO members but also illustrates a critical aspect of the development in today's cyber security landscape that seems to move towards a "nation-centric" paradigm. Cyber, as the fifth domain of warfare, needs specific CBMs that requires significant commitment from negotiating states. Such measures have been the basis for the adoption of the BWC for instance, and have been flagged as prerequisite by UNGGE, NATO, and the European Union, whilst the SCO states have inserted them in the code of conduct. Questions regarding codes of conduct in the cyber offensive action domain have been raised starting from the EU to NATO. The recent exploration of a Permanent Structured Cooperation on security and defence

[103] Henry Rõigas, "An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?", in *Incyder News*, 10 February 2015, https://ccdcoe.org/node/539.html.

[104] Europol, *Are You Sharing the Same IP Address As a Criminal? Law Enforcement Call for the End of Carrier Grade NAT (CGN) to Increase Accountability Online*, 17 October 2017, https://www.europol.europa.eu/node/2427.

ISSN 2280-6164

(PESCO), which explicitly aims to reinforce EU strategic autonomy,[105] could provide the institutional ground for a code of conduct. This is essential to avoid a double-track defence policy, characterized by an EU cooperative effort in the classic domain of warfare and a cyber domain limited to a national-only approach.

Furthermore, OSCE could serve as a multilateral platform to achieve a consensus, which can then be built upon within the UN Security Council. It is certainly hard to keep nation states from establishing offensive cyber capabilities, since the process is already on-going and no international law can deny a nation state the ability to build its own army for defensive purposes. Although lobbying on CBMs appears to be the most valuable and achievable way to ensure security in cyber space, efforts can still encourage a defensive approach rather than offensive. This also represents an opportunity for the EU to strengthen its role in the international arena because limiting the scope of policy activities within the EU in such an interconnected world may be insufficient. Transparency on cyber units should be a "must" among nation states, as well as sharing a common doctrine for it too. A common doctrinal effort to include cyber operations within the range of warfare actions is needed to clarify the sequential steps of engagement. This could be directly connected, for example, to nuclear dissuasion, as cyber-attacks can no longer be conceived as limited to the cyber domain. Thus, the sharing of doctrines can contribute to the creation of a global cyber trust environment.

Another topic which needs to be examined, and on which the UNGGE failed to find consensus, is the lawfulness of response to an attack.[106] If a nation state is the victim of a cyber-attack, under which circumstances should that nation be able to respond by harming the structure of the attacking state? This unresolved question has strong links with the attribution problem and the proxy state issue: it may be difficult to identify who is responsible for an attack, or the attacker may use proxy states for the waging of the attack. The United States' position on the matter is that any international treaty should include an option to respond to attacks. Article 51 of the UN Charter affirms the "right of individual self-defence" and a vast jurisprudence has been created on the matter by the International Court of Justice and international tribunals. On the other hand, the Cuban delegation within the UNGGE, with the support of the Chinese and Russian delegations, expressed concerns about the militarization of cyber space, which would, in their opinion, occur in the case of recognition of a right of self-defence.[107] NATO recognition in the cyber pledge of cyber space as the fifth domain of warfare already gives a clear hint on how the western countries, which are part of the treaty, deal with the idea of cyber defence. Does it therefore make sense to deny a right of self-defence while

[105] European External Action Service (EEAS), *Permanent Structured Cooperation (PESCO) - Factsheet*, 5 March 2018, http://europa.eu/!fY63Tc.

[106] Stefan Soesanto and Fosca D'Incau, "The UN GGE Is Dead: Time to Fall Forward", in *ECFR Commentaries*, 15 August 2017, http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.

[107] Miguel Rodrìguez, *Declaration by the Representative of Cuba*, cit.

ISSN 2280-6164

half of the world is preparing to defend its cyber borders through military units tasked for this? The answer may be found in the lemma "active defence", a concept which is being implemented *inter alia* by the European Defence Agency (EDA).[108] Through the definition of active defence, the agency proposes several measures to respond to attacks without intrusive action.

Another tricky topic when dealing with cyber space, is the dual-use and related export control issue. Experts remain divided about the value of agreements such as the Wassenaar Arrangement. Although there is a general consensus on the fact that the spreading of cyber weapons, intrusion software, and malicious operations should be avoided, there is no agreement about the method to reach such a goal. Export control regimes have been partially successful in avoiding the proliferation of weapons of mass destruction in many fields as demonstrated by the nuclear or the biological experience. A delicate and technology-based domain, such as cyber space, needs independent experts to work closely on the negotiations among nation states for export control. Several interviews conducted for this study underlined that a partially incorrect choice to include certain cyber security tools in lists of export control for dual-use items may pose a risk to information sharing as regards malicious software. Information sharing is a key issue, being at the base of CBMs strategies and of many declarations and documents issued by the UNGGE, EU, NATO and OSCE.

The question of export control is linked to the role of the private sector as well. Up until now, the private sector and the CERTs are the first respondents in case of incidents. The international community may not be able to adequately secure cyber space without a common mechanism when private companies are owners of most of the technologies and infrastructure in cyber space. Further analysis and debate is essential for the definition of a framework of actions between private companies and nation states or multilateral organizations. The role of the private sector and a common mechanism for nation states should be analysed in the light of an application of existing international law, so as to organize them through a more comprehensive effort. The question of cyber conflict regulation is therefore raised.

4.1 A regulation of offensive behaviours in cyber space

Our report concerning the possibility for a future codification of nation-state offensive behaviour in cyber space has as a primary assumption in the idea that cyber conflict can be the subject of international law. In this respect, the applicability of international law in cyber space has been widely accepted (though not by all) in the international community.[109] For example, the US' 2011 "International Strategy

[108] See EDA website, *Cyber Defence*, 5 September 2017, https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence.

[109] Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", in *Harvard International Law Journal Online*, Vol. 54 (December 2012), p. 13-37, http://

ISSN 2280-6164

for Cyber space" underlines that "[t]he development of norms for state conduct in cyber space does not require a reinvention of customary international law. Long-standing international norms guiding state behaviour – in times of peace and conflict – also apply in cyber space".[110]

This interpretation was supported by the UNGGE that affirmed the existence of obligations in cyber space under international law in the framework of the agreement signed in June 2015. Furthermore, NATO's Cyber Defence Pledge focuses on the reaffirmation of the applicability of international law in cyber space. Finally, the most important document in that field is clearly the Tallinn Manual, which underlines the main aspects of such application.

This application has been widely supported by the international community, including in the 1977 Additional Protocol I to the 1949 Geneva Conventions: "[i]n cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience".[111] In other words, IHL accommodates the development of new technology and is sufficiently flexible to adapt to the global state of the art. Thus, cyber weapons, as with other new weapons, are subject to pre-existing law.

However, the applicability of IHL to cyber operations was discussed during the 2016/2017 UNGGE meeting without reaching a consensus. From the perspective of Cuba, supported by Russia and China, "the supposed applicability in the context of ICT of the principles of international humanitarian law [...] would legitimize a scenario of war and military actions in the context of ICT".[112] This is juxtaposed when compared to the application of international humanitarian law (IHL) to new means and methods of warfare. Therefore, for a future international agreement on cyber space it would be indispensable for the international community to reach a consensus over the application of IHL to the cyber domain. Without such a common vision, the overall stability of international peace and security would be constantly undermined by uncertainty over the consequences of the behaviour of nation states in cyber space. Additionally, discussion is ongoing as regards the suitability of the principles of division, proportionality and precautions. The main concerns which appear throughout the analysis that need be scrutinized by policy-makers, include the abundance of dual-use technologies in cyber space and the indirect or unintended consequences and collateral damage from a cyber-attack. Because of those two specific features, applying IHL core principles is substantially

www.harvardilj.org/?p=6187.

[110] White House, *International Strategy for Cyberspace*, May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

[111] Art. 1(2) of the Additional Protocol (I) to the Geneva Conventions, cit.

[112] Miguel Rodrìguez, *Declaration by the Representative of Cuba*, cit. See also Michael N. Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms", in *Just Security Articles*, 30 June 2017, https://wp.me/p5gGh3-b7O.

ISSN 2280-6164

harder than in a kinetic attack.

In cyber space, dual-use material encounters the difficulty of separately identifying military and civilian objects. As a result, both the division and precautions principles cannot be successfully applied. Although the separation between military and civilian objects is an essential element of IHL, this is not the case in practice because nation states have not applied it in the same way to civilian systems.[113] Even though these concerns are shared by different scholars, the Tallinn International Group of Experts did not evaluate it as uniquely problematic. In fact, the dual-use "dilemma" can be resolved by considering a military objective as anything used for military purposes. According to the Tallinn Manual, "The analogy is a road network used by both military and civilian vehicles. Although an attacker may not know with certainty which roads will be travelled by enemy military forces [...] the network is a military objective subject to attack. There is no reason to treat computer networks differently".[114] However, the UNGGE highlights the relevance of the evaluation of the means used to carry out an attack in view of the principles of proportionality and precautions.

The issue of dual-use technologies within the cyber domain therefore poses important challenges to the applicability of IHL to cyber space. An international framework could address this by preventing nation states from concluding that the entire Internet can be considered a military objective.

4.2 The need for the protection of civilians from cyber-attacks

Another major challenge to the application of IHL to cyber space is the effects of indirect or unintended consequences and collateral damage that increase in cyber space. UNGGE has underlined how such effects on civilian systems must be factored into the interpretation of the proportionality principle.[115] Generally, the risk of such effects from a cyber-attack is widely recognized by the international community. Legal standards for kinetic operations would also be valid for cyber operations. In fact, even if it would be increasingly challenging to conduct cyber operations in respect of the principles of precaution and proportionality, no significant addition to the standard targeting analysis would be required.[116]

As an example of regional cooperation, the European Union has recently launched the European Defence Fund (EDF), whose objective is the integration of national defence sectors. By 2019, the Union plans to allocate 90 million euros to stimulate collaborative research in defence technology.[117] This strategy emphasizes the need

[113] Robin Geiß and Henning Lahmann, "Cyber Warfare", cit.
[114] Michael N. Schmitt (ed.), *Tallinn Manual 2.0*, cit., p. 446.
[115] Michael N. Schmitt, "International Law in Cyberspace", cit.
[116] Eric Talbot Jensen, "Unexpected Consequences from Knock-on Effects", cit.
[117] Alessandro Ungaro, "Difesa europea: ora tocca agli Stati", in *AffarInternazionali*, 16 June 2017, http://www.affarinternazionali.it/?p=65044.

ISSN 2280-6164

for nation states to face increasing international threats together. The scope of any EU effort for cooperation and collaboration between member states in the defence sector integration could easily be broadened to include cyber space, functioning as a concrete example of the advantages of such a strategy. Collaboration and information sharing is fundamental, both internally amongst national institutions and also externally between nation states. The containment of any cyber threat would be ineffective without such collaboration and information sharing. Considering the pervasive nature of the threats from cyber-attacks, and the fact that they can come from different sources, no single central authority would be powerful enough or have the necessary amount of information to assure adequate stability of international peace and security.

A permanent collaboration between nation states and legal and cyber security experts is needed for appropriate action to be taken in cyber space. Military orders should always consider such expert opinions before launching a cyber-attack and nation states should also constantly collaborate. The above-mentioned CERT-EU and ENISA centres are only two of the positive examples of such collaboration. Both institutions are contributing in the creation of a network of expertise around Europe. A strengthened and increased number of such collaboration initiatives, including organizations outside the European Union, would represent a further step towards a common definition of strategies and policies. Clearly, these two aspects, information sharing and experts' collaboration, are fundamentally interrelated and often overlap in terms of practical implementation.

4.3 Cooperation between the public and private sectors and cross-industry collaboration

Greater cooperation between the public and private sectors could also help to guarantee the resilience of network and information systems in cases of cyber-attacks. In fact, the private sector is one of the main actors responsible for ensuring security in cyber space. For the first time in history, we are witnessing an important change in the relationship between nation states and non-state actors, where the private sector has been progressively integrated through public-private sector cooperation into the collective management of cyber security. Both the NATO Industry Cyber Partnership and the NIS Directive engage the private sector in a regular exchange of information and expertise that allows the collection of technical assets necessary for an improved, global level of cyber security. While States should engage in a constructive discussion around the need for international rules, industry should deepen its efforts to agree upon and develop a set of "industry-norms". These could include a set of principles and codes of conduct for collaborating in response to cyber-attacks and ensuring industry does not support any governments in conducting cyber-attacks, etc.

While all these issues must be carefully taken in consideration in the application of IHL to cyber space, the report has shown that perspectives for such application are concrete. Although the international community will have to face multiple challenges, there are no concrete limitations to the application of existing

ISSN 2280-6164

international regulation to cyber space. The Tallinn Manual has proven to be an important starting point in this direction. On the other hand, the prospective of creating an arms control treaty on the blueprint of the NPT, BWC and CWC presents several difficulties: (a) the problem of finding a compliance checking mechanism to the treaty; and (b) cyber-attack attribution.

4.4 Compliance mechanisms and cyber-attack attribution

Attribution is critical to the resolution of many cyber security challenges.[118] On the one hand, attribution imposes responsibility and helps to ensure compliance with the agreed upon norms in the 2015 UNGGE report; on the other hand, attribution deters future cyber-attacks by raising the cost of cyber activities. The issue of attribution is therefore a serious challenge that governments should address urgently, such as through the creation or support of an international attribution organization that could analyse breaches in the 2015 UNGGE norms or work to improve attribution capacity for countries.

In particular, the challenge of reaching a high confidence of attribution in a timely manner is especially difficult. It is true that some of the inherent features of cyber space complicate the ability to access, interpret, and compare digital evidence. Three inherent features of cyber space make the attribution challenge particularly difficult to overcome: (a) the secrecy and plausible deniability of a cyber-attack; (b) the possibility of launching a sustained, multi-stage cyber-attack known as Advanced Persistent Threat (APT);[119] and (c) the speed with which a cyber-attack can materialize.[120]

When governments deal with attribution, they must be able to distinguish the process into two phases: technical attribution, i.e. the identification and the localization of the source node which initiated the attack, and human attribution using the result of technical attribution in combination with intelligence and information analysis to identify the actual actor responsible for the cyber-attack. Cyber space enables actors to operate with various degrees of anonymity, making

[118] For more on the attribution issue please see, John P. Carlin, "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats", in *Harvard National Security Journal*, Vol. 7, No. 2 (2016), p. 391-436, http://harvardnsj.org/wp-content/uploads/2016/06/Carlin-FINAL.pdf; David A. Wheeler and Gregory N. Larsen, "Techniques for Cyber Attack Attribution", in *IDA Papers*, No. P-3792 (October 2003), http://www.dtic.mil/docs/citations/ADA468859; and Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack", in *Journal of Cybersecurity*, Vol. 1, No. 1 (September 2015), p. 53-67, https://doi.org/10.1093/cybsec/tyv003.

[119] Kuldeep Singh, Priyanka Singh and Pradeep Kumar Singh, "Review of Multistage Cyber Attack", in *International Journal of Engineering Applied Science and Technology*, Vol. 1, No. 1 (2015), p. 19-23, http://www.ijeast.com/papers/20-24,Tesma101,IJEAST.pdf.

[120] Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations", in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds.), *4th International Conference on Cyber Conflict. Proceedings 2012*, Tallinn, NATO CCDCOE, 2012, p. 91-109, http://www.ccdcoe.org/node/378.html.

ISSN 2280-6164

attribution much more complicated than in the physical world. For instance, even when the registration of a machine is known, the current physical location of the machine may be difficult to determine (since the machine may be portable and accessing the Internet over long-distance telecommunication).[121]

Once technical attribution has been accomplished, it is necessary to identify who conducted the cyber-attack. In cyber space it is difficult to determine whether malicious actors are acting on behalf of nation states, independent criminal groups, or even individuals. Therefore, human attribution is essential to identify the cyber-attacker. Together with intelligence data and other analysis of the political context, cyber security analysts can trace back the planner of the attack.[122] It is important to mention that recent cyber-attacks, such as Wannacry, have shown frequent similarities, which enable investigators to link different incidents to the same actors. In other words, past investigations affect current attribution assessments, and attribution investigations must track actors over the course of their varied activity, potentially over several years.

Communicating attribution also presents the challenge of "second phase" attribution. Communicating an attribution finding to the general public represents the real difficulty for governments, who even if able to trace criminals have trouble expressing credible accusations. There are many examples that show how public statements of an attribution finding are often not perceived as credible or persuasive. It is a multi-layered problem and derives from different causes. The creation of an independent attribution organization developing a trustworthy reputation would bring greater credibility to assertions of attribution on the origin of a cyber-attack.

The combined effect of the described challenges related to issues of verification and attribution suggest that an arms control treaty for cyber weapons may not be effective. The application of existing provisions of IHL seem, under the current circumstances, more appropriate. Any future non-proliferation regime for cyber weapons will demand greater commitment of nation states.

Conclusions

The review of existing arms control treaties and of the Geneva Conventions analysed in the second chapter, together with the ongoing initiatives in cyber space, have highlighted several topics of interest treated in the fourth chapter. The study achieved a broad scope rather than researching each issue in detail. Nevertheless

[121] W. Earl Boebert, "A Survey of Challenges in Attribution", in Committee on Deterring Cyberattacks, *Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy*, Washington, The National Academies Press, 2010, p. 41-52, https://www.nap.edu/read/12997/chapter/5.

[122] Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution", in *Journal of Conflict & Security Law*, Vol. 17, No. 2 (2012), p. 229-244, https://ssrn.com/abstract=2538271.

ISSN 2280-6164

we have conducted an initial analysis that can prompt useful debate that could be further developed in future research. We believe that this contribution to the debate on cyber weapons control is important to enhance the awareness of risks from the spread of cyber threats. Although we feel that technological development is an important condition for a better society in future, it is equally important to research and highlight concerns about the misuse of technology.

It seems clear that the military forces of the most powerful countries in the world are committed to the creation of units with a cyber focus. Over the coming years, this cyber arms race will pose increasing threats to the stability of international peace and security. In this context, nation states are recognizing the need for a common agreement on the regulation of cyber space and cyber-offensive behaviours. This is demonstrated by the numerous agreements and initiatives undertaken under the UN and by regional organizations such as OSCE, EU, and NATO. Starting from these assumptions, our investigation on the applicability of the fourth Geneva Convention to cyber space also points in the right direction. Cyber-offensive behaviours can potentially fall under IHL provisions, specifically when dealing with protection of civilian populations and civilian infrastructures. However, IHL adaptability and adjustments to the specificities of cyber weapons need greater consensus internationally. Further discussions and research on international law and guidance, such as the Tallinn Manual, should be supported and sponsored by nation states.

In addition, the risks produced by the spread of cyber threats can be mitigated by an international non-proliferation agreement, like the ones regulating nuclear, biological and chemical weapons. Similarly, a binding agreement requires essential elements of common definitions, and trust.

First of all, definitions matter and although a provision may seem obvious, the international community still lacks a common vocabulary for cyber space that could be the basis for an agreement. This has been evident in the experience of the UNGGE and of proposed agreements within the UN, while vocabulary has not been a main concern in existing treaties. Trust is another essential element due to the nature of cyber space and development of an information sharing agreement could follow the same approach as development of confidence-building measures by engendering greater trust between nation states through information sharing initiatives.

Further evidence from inputs to this study show that a second requirement for a common vocabulary is a definition regarding the threshold for recognizing a cyber-attack as a "use of force" or "armed conflict" under international humanitarian law. This was a significant obstacle to consensus for the UNGGE and also one of the most debated issues within defensive organizations, such as NATO, as well as clear agreement on the boundary between active defence and offensive actions. Active defence is among the grey areas in which the boundaries are not yet commonly defined. Among the unsolved questions lies the attribution of an attack.

ISSN 2280-6164

Considering the responsibilities and commitments of private companies in the governance of the Internet, they should be included in the discussions and in the implementation of binding agreements on the acceptable behaviour of nation states in cyber space. The further cooperation between the public and private sector is vital for the validity of an international regime of non-proliferation of cyber weapons because any absence of private companies would imply a lack of coherence in the scope of such a regime.

While new technologies are working towards a resolution of such issues and would allow us to overcome this problem soon, political implications of attribution seem far from resolved. These issues could be addressed through the creation within the international agreement of an attribution organization. Such an agreement can be successful only if participants are committed to giving it a strong authority, along the same lines of IAEA. The work of an attribution organization should be practical and achieved through national representatives/inspectors from nation states together with neutral, third-party, international, technical experts in cyber security from the private sector, and whose accountability should be internationally accepted through provisions of a binding international agreement. The tasks foreseen for this organization would be to: (a) define a common vocabulary among international stakeholders; (b) establish the boundaries between active defence and offensive cyber behaviours; (c) delineate a threshold for recognizing a cyber-attack as a "use of force" or "armed conflict" under international humanitarian law; and (d) attribute the eventual attack to a State through a shared decision.

An attribution organization could not be created by a single nation state or even a small group of countries. It needs an international discussion which should also be supported by public awareness of the matter and consequently by civil society. Although the goal for this organization could not be to completely eradicate future cyber weapons among the spectrum of possible offensive tools, which is the aim of existing non-proliferation treaties, the regulation of formal, international attribution is increasingly necessary due to recent worldwide cyber-attacks. Beginning such negotiations would be the most promising action in advancing the issue of cyber arms control.

Updated 15 March 2018

ISSN 2280-6164

References

Additional Protocol (I) to the Geneva Conventions, 1977, https://ihl-databases.icrc.org/ihl/INTRO/470

Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations", in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds.), *4th International Conference on Cyber Conflict. Proceedings 2012*, Tallinn, NATO CCDCOE, 2012, p. 91-109, http://www.ccdcoe.org/node/378.html

ASEAN Regional Forum, *ARF Work Plan on Security of and in the Use of Information and Communications Technologies*, 7 May 2017, http://aseanregionalforum.asean.org/events/3-content/public-library/665-plan-of-action-and-work-plans.html

Hannah Beech, "Meet China's Newest Soldiers: An Online Blue Army", in *Time*, 27 May 2011, https://wp.me/p1lnq5-1fy

Richard K. Betts, "Systems for Peace or Causes of War? Collective Security, Arms Control, and the New Europe", in *International Security*, Vol. 17, No. 1 (Summer 1992), p. 5-43

W. Earl Boebert, "A Survey of Challenges in Attribution", in Committee on Deterring Cyberattacks, *Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy*, Washington, The National Academies Press, 2010, p. 41-52, https://www.nap.edu/read/12997/chapter/5

Gil Bousquet, "Paris et Berlin déploient leurs cyber-soldats", in *La Dépêche*, 17 December 2016, https://www.ladepeche.fr/article/2016/12/17/2481004-paris-et-berlin-deploient-leurs-cyber-soldats.html

Eric Boylan, "Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners", in *Vanderbilt Journal of Transnational Law*, Vol. 50, No. 1 (February 2017), p. 217-244, https://www.vanderbilt.edu/jotl/2017/02/applying-the-law-of-proportionality-to-cyber-conflict-suggestions-for-practitioners

John P. Carlin, "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats", in *Harvard National Security Journal*, Vol. 7, No. 2 (2016), p. 391-436, http://harvardnsj.org/wp-content/uploads/2016/06/Carlin-FINAL.pdf

Jeffrey Carr, "The Misunderstood Acronym: Why Cyber Weapons aren't WMD", in *Bulletin of the Atomic Scientists*, Vol. 69, No. 5 (2013), p. 32-37

China's Ministry of National Defense, *China's Military Strategy*, May 2015, http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm

ISSN 2280-6164

James R. Clapper, Marcel Lettre and Michael S. Rogers, *Foreign Cyber Threats to the United States*, Joint Statement for the Record to the Senate Armed Services Committee, 5 January 2017, https://www.armed-services.senate.gov/download/clapper-lettre-rogers_01-05-17

Richard A. Clarke and Robert K. Knake, *Cyber War. The Next Threat to National Security and What to Do about It*, New York, HarperCollins, 2010

Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare", in *CNA Occasional Papers*, March 2017, https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf

Andrew P. Cortell and James W. Davis, "How Do International Institutions Matter? The Domestic Impact of International Rules and Norms", in *International Studies Quarterly*, Vol. 40, No. 4 (December 1996), p. 451-478

Council of the European Union, *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* (9916/17), 7 June 2017, http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

Council of the European Union, *Horizontal Working Group on Cyber Issues - Establishment and adoption of its Terms of Reference* (13114/16), 20 October 2016, http://data.consilium.europa.eu/doc/document/ST-13114-2016-INIT/en/pdf

David Davenport, "The New Diplomacy", in *Policy Review*, No. 116 (December 2002/January 2003), p. 17-30, https://www.heritage.org/node/18600

Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians", in *International Review of the Red Cross*, Vol. 94, No. 886 (Summer 2012), p. 533-578, https://www.icrc.org/eng/assets/files/review/2012/irrc-886-droege.pdf

European Commission, *Assessment of the EU 2013 Cybersecurity Strategy* (SWD/2017/295), 13 September 2017, https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF

European Commission, *Commission Recommendation (EU) 2017/1584 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises* (C/2017/6100), 13 September 2017, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32017H1584

European Commission, *Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")* (COM/2017/477/3), 22 February 2018, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52017PC0477R(02)

ISSN 2280-6164

European External Action Service (EEAS), *Permanent Structured Cooperation (PESCO) - Factsheet*, 5 March 2018, http://europa.eu/!fY63Tc

Europol, *Are You Sharing the Same IP Address As a Criminal? Law Enforcement Call for the End of Carrier Grade NAT (CGN) to Increase Accountability Online*, 17 October 2017, https://www.europol.europa.eu/node/2427

France's Government, *French White Paper on Defence and National Security 2013. Twelve Key Points*, July 2013, http://www.defense.gouv.fr/actualites/articles/livre-blanc-2013

France's Ministry of Defence, *Déclaration de M. Jean-Yves Le Drian, ministre de la défense, sur la cyberdéfense*, Bruz, 12 December 2016, http://discours.vie-publique.fr/notices/163003632.html

G20 Leaders' Communiqué, Antalya, 16 November 2015, http://www.g20.utoronto.ca/2015/151116-communique.html

Daniel Garrie and Shane R. Reeves, "An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors", in *Cardozo Law Review*, Vol. 37, No. 5 (2016), p. 1827-1866, http://www.cardozolawreview.com/content/37-5/GARRIE.REEVES.37.5.pdf

Robin Geiß and Henning Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space", in *Israel Law Review*, Vol. 45, No. 3 (November 2012), p. 381-399, https://core.ac.uk/download/pdf/16457774.pdf

Geneva Convention (IV) on Civilians, 1949, https://ihl-databases.icrc.org/ihl/INTRO/380

Keir Giles, "'Information Troops' – a Russian Cyber Command?", in Christian Czosseck, Enn Tyugu and Thomas Wingfield (eds.), *3rd International Conference on Cyber Conflict. Proceedings 2011*, Tallinn, NATO CCDCOE, 2011, p. 45-60, https://ccdcoe.org/node/375.html

Keir Giles, "Russia's Public Stance on Cyberspace Issues", in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds.), *4th International Conference on Cyber Conflict. Proceedings 2012*, Tallinn, NATO CCDCOE, 2012, p. 63-75, http://www.ccdcoe.org/node/378.html

James B. Godwin et al. (eds.), "The Russia-U.S. Bilateral on Cybersecurity. Critical Terminology Foundations 2", in *EastWest Institute Policy Reports*, No. 2/2014 (March 2014), https://www.files.ethz.ch/isn/178418/terminology2.pdf

Justyna Gotkowska, "The Cyber and Information Space: A New Formation in the Bundeswehr", in *OSW Analyses*, 12 April 2017, https://www.osw.waw.pl/en/publikacje/analyses/2017-04-12/cyber-and-information-space-a-new-

ISSN 2280-6164

formation-bundeswehr

Claudio Graziano, "Cyber Defence. The Joint Cyber Command is Born", Interview with the Chief of Defence Staff in *Informazioni della Difesa*, No. 3/2017, p. 12-15, https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/cyber_defence.pdf

Katriina Härmä and Tomáš Minárik, "European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox", in *Incyder News*, 18 September 2017, https://ccdcoe.org/node/1221.html

Emily Haslam, "Information Warfare: Technological Changes and International Law", in *Journal of Conflict and Security Law*, Vol. 5, No. 2 (December 2000), p. 157-175

Emilio Iasiello, "Are Cyber Weapons Effective Military Tools?", in *Military and Strategic Affairs*, Vol. 7, No. 1 (March 2015), p. 23-39, http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/SystemFiles/2_Iasiello.pdf

International Committee of the Red Cross (ICRC), *Conference of the States Parties to the Chemical Weapons Convention: statement by the ICRC*, 30 November 2016, https://www.icrc.org/en/document/conference-chemical-weapons-convention-2016

International Committee of the Red Cross (ICRC), "How is the Term 'Armed Conflict' Defined in International Humanitarian Law?", in *ICRC Opinion Papers*, 17 March 2008, https://www.icrc.org/eng/resources/documents/article/other/armed-conflict-article-170308.htm

International Court of Justice (ICJ), *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*, 8 July 1996, http://www.icj-cij.org/en/case/95/advisory-opinions

International Criminal Tribunal for the former Yugoslavia (ICTY), Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction in Case No. IT-94-1, *Prosecutor v. Dućko Tadić*, 2 October 1995, http://www.icty.org/x/cases/tadic/acdec/en/51002.htm

Eric Talbot Jensen, "Cyber Attacks: Proportionality and Precautions in Attack", in *Naval War College International Law Studies*, Vol. 89 (2013), p. 198-217, http://digital-commons.usnwc.edu/ils/vol89/iss1/15

Eric Talbot Jensen, "Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations", in *American University International Law Review*, Vol. 18, No. 5 (2003), p. 1145-1188, http://digitalcommons.wcl.american.edu/auilr/vol18/iss5/3

Andrew Jones and Gerald L. Kovacich, *Global Information Warfare. The New Digital Battlefield*, 2nd ed., Boca Raton, CRC Press, 2016

ISSN 2280-6164

John J. Kelly and Lauri Almann, "eWMDs", in *Policy Review*, No. 152 (December 2008/January 2009), p. 39-50, http://www.modelsoftware.com/people/152KellyAlmannOffprint.pdf

Richard Kissel (ed.), "Glossary of Key Information Security Terms", in *NIST Interagency/Internal Report (NISTIR)*, No. 7298rev2 (May 2013), https://www.nist.gov/node/579721

Elaine Korzak, "UN GGE on Cybersecurity: The End of an Era?", in *The Diplomat*, 31 July 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe

Valérie Leroux, "Les armées françaises intègrent le combat numérique à leur arsenal", in *AFP*, 12 December 2016, https://fr.news.yahoo.com/armées-françaises-intègrent-combat-numérique-à-arsenal-115324176.html

Kalev Letaruu, "What Tallinn Manual 2.0 Teaches Us about the New Cyber Order", in *Forbes*, 9 February 2017, https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order

James Andrew Lewis and Götz Neuneck, *The Cyber Index. International Security Trends and Realities*, New York and Geneva, United Nations, 2013, http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Stephanie Liechtenstein, "The OSCE's Pioneering Work on Cyber Security", in *Security and Human Rights Monitor*, 4 April 2016, https://www.shrmonitor.org/osces-pioneering-work-cyber-security

Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack", in *Journal of Cybersecurity*, Vol. 1, No. 1 (September 2015), p. 53-67, https://doi.org/10.1093/cybsec/tyv003

Mandiant, *APT 1. Exposing One of China's Cyber Espionage Units*, February 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Michele G. Markoff, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, Remarks by the US Department of State Deputy Coordinator for Cyber Issues, New York, 23 June 2017, https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm

Markus Maybaum and Jens Tölle, "Arms Control in Cyberspace – Architecture for a Trust-Based Implementation Framework Based on Conventional Arms Control Methods", in Nikolaos Pissanidis, Henry Rõigas and Matthijs Veenendaal (eds.), *8th International Conference on Cyber Conflict. Proceedings 2016*, Tallinn, NATO CCDCOE, 2016, p. 159-173, https://ccdcoe.org/node/1039.html

ISSN 2280-6164

Joe McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy", in *China Briefs*, Vol. 15, No. 8 (17 April 2015), p. 3-6, https://jamestown.org/?p=12824

Steven Lee Myers, "Youth Groups Created by Kremlin Serve Putin's Cause", in *The New York Times*, 8 July 2007, https://nyti.ms/2tgvBE0

NATO, *Cyber Defence Pledge*, 8 July 2016, https://www.nato.int/cps/su/natohq/official_texts_133177.htm

NATO, *NATO and the European Union Enhance Cyber Defence Cooperation*, 10 February 2017, https://www.nato.int/cps/en/natohq/news_127836.htm

Joseph S. Nye Jr., *The Future of Power*, New York, PublicAffairs, 2011

Organization for the Prohibition of Chemical Weapons (OPCW), *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction* (Chemical Weapons Convention), 13 January 1993, https://www.opcw.org/chemical-weapons-convention

Organization for Security and Co-operation in Europe (OSCE), *Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies* (PC.DEC/1106), 3 December 2013, http://www.osce.org/pc/109168

Organization for Security and Co-operation in Europe (OSCE), *Decision No. 1202: OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies* (PC.DEC/1202), 10 March 2016, https://www.osce.org/pc/227281

Organization of the American States (OSA), *Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity* (AG/RES. 2004 (XXXIV-O/04)), 8 June 2004, http://www.oas.org/xxxivga/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

Patryk Pawlak, "Confidence-Building Measures in Cyberspace: Current Debates and Trends", in Anna-Maria Osula and Henry Rõigas (eds.), *International Cyber Norms. Legal, Policy & Industry Perspectives*, Tallinn, NATO CCDCOE, 2016, p. 129-153, https://ccdcoe.org/node/956.html

Cheryl Pellerin, "DARPA's Plan X Gives Military Operators a Place to Wage Cyber Warfare", in *DoD News*, 12 May 2016, https://www.defense.gov/News/Article/Article/758219

ISSN 2280-6164

Jean S. Pictet (ed.), *Commentary on the Geneva Conventions of 12 August 1949, Vol. 4: Geneva Convention relative to the Protection of Civilian Persons in Time of War*, Geneva, ICRC, 1958, https://www.loc.gov/rr/frd/Military_Law/pdf/GC_1949-IV.pdf

Laura Reed, *Weapons of Mass Destruction*, Hampshire College Peace and World Security Studies: Conflict Topics, https://www.hampshire.edu/node/35664

Tom Reeve, "France Unveils Cyber Command in Response to 'New Era in Warfare'", in *SC Media*, 16 December 2016, https://www.scmagazineuk.com/france-unveils-cyber-command-in-response-to-new-era-in-warfare/article/579671

Miguel Rodrìguez, *Declaration by the Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 23 June 2017, https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf

Henry Rõigas, "An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?", in *Incyder News*, 10 February 2015, https://ccdcoe.org/node/539.html

Russia's Ministry of Foreign Affairs, *Convention on International Information Security*, 22 September 2011, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

Michael S. Schmidt and David E. Sanger, "5 in China Army Face U.S. Charges of Cyberattacks", in *The New York Times*, 19 May 2014, https://nyti.ms/2FDiqQm

Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", in *Harvard International Law Journal Online*, Vol. 54 (December 2012), p. 13-37, http://www.harvardilj.org/?p=6187

Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013

Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, Cambridge University Press, 2017

Michael N. Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms", in *Just Security Articles*, 30 June 2017, https://wp.me/p5gGh3-b7O

Thomas Shea, Sandro Gaycken and Maurizio Martellini, "Cyber Security for Nuclear Power Plants", in Maurizio Martellini (ed.), *Cyber Security. Deterrence and IT Protection for Critical Infrastructures*, Cham, Springer, 2013, p. 25-35

ISSN 2280-6164

Kuldeep Singh, Priyanka Singh and Pradeep Kumar Singh, "Review of Multistage Cyber Attack", in *International Journal of Engineering Applied Science and Technology*, Vol. 1, No. 1 (2015), p. 19-23, http://www.ijeast.com/papers/20-24,Tesma101,IJEAST.pdf

David J. Smith, "How Russia Harnesses Cyberwarfare", in *AFPC Defense Dossier*, No. 4 (August 2012), p. 7-11, http://www.afpc.org/files/august2012.pdf

Stefan Soesanto and Fosca D'Incau, "The UN GGE Is Dead: Time to Fall Forward", in *ECFR Commentaries*, 15 August 2017, http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance

John Stone, "Cyber War Will Take Place!", in *Journal of Strategic Studies*, Vol. 36, No. 1 (2013), p. 101-108

Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution", in *Journal of Conflict & Security Law*, Vol. 17, No. 2 (2012), p. 229-244, https://ssrn.com/abstract=2538271

UK Government, *National Cyber Security Strategy 2016-2021*, November 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

UK Government, *National Security Strategy and Strategic Defence and Security Review 2015*, November 2015, https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015

UK House of Commons Defence Committee, *Defence and Cyber-security. Written Evidence*, February 2012, https://publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/1881.pdf

UK Ministry of Defence, *Defence Secretary's speech at Cyber 2017 Chatham House Conference*, 27 June 2017, https://www.gov.uk/government/speeches/defence-secretarys-speech-at-cyber-2017-chatham-house-conference

UN Disarmament Commission, *Special Report of the Disarmament Commission to the General Assembly on its Third Special Session devoted to Disarmament* (A/S-15/3), 28 May 1988, https://s3.amazonaws.com/unoda-web/documents/library/AS-15_3.pdf

UN General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* (A/66/359), 14 September 2011, http://undocs.org/A/66/359

ISSN 2280-6164

UN General Assembly, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* (A/69/723), 13 January 2015, http://undocs.org/A/69/723

UN General Assembly, *Resolution on the Developments in the field of information and telecommunications in the context of international security* (A/RES/53/70), 4 January 1999, http://undocs.org/A/RES/53/70

UN Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/60/202), 5 August 2005, http://undocs.org/A/60/202

UN Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174), 22 July 2015, http://undocs.org/A/70/174

Alessandro Ungaro, "Difesa europea: ora tocca agli Stati", in *AffarInternazionali*, 16 June 2017, http://www.affarinternazionali.it/?p=65044

US Bureau of Industry and Security, "Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items", in *US Federal Register*, Vol. 80, No. 97 (20 May 2015), p. 28853-28863, https://www.federalregister.gov/d/2015-11642

US Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, January 2018, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Jennifer Valentino-DeVries, Lam Thuy Vo and Danny Yadron, "Cataloging the World's Cyberforces", in *The Wall Street Journal*, 28 December 2015, http://graphics.wsj.com/world-catalogue-cyberwar-tools

Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities. Cyber Conflict in the International System*, Oxford, Oxford University Press, 2015

Nina Werkhäuser, "German Army Launches New Cyber Command", in *Deutsche Welle*, 1 April 2017, http://p.dw.com/p/2aTfJ

David A. Wheeler and Gregory N. Larsen, "Techniques for Cyber Attack Attribution", in *IDA Papers*, No. P-3792 (October 2003), http://www.dtic.mil/docs/citations/ADA468859

White House, *International Strategy for Cyberspace*, May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

ISSN 2280-6164

White House, *Statement by President Donald J. Trump on the Elevation of Cyber Command*, 18 August 2017, https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command

Clay Wilson, "Cybersecurity and Cyber Weapons: Is Nonproliferation Possible?", in Maurizio Martellini (ed.), *Cyber Security. Deterrence and IT Protection for Critical Infrastructures*, Cham, Springer, 2013, p. 11-24

Andrew Woodcock, "Boris Johnson Tells Russia to Halt Cyber Attacks on the West during Visit to Moscow", in *The Indipendent*, 22 December 2017, http://www.independent.co.uk/news/uk/politics/boris-johnson-russia-latest-cyber-attacks-putin-moscow-a8123681.html

ISSN 2280-6164

ISSN 2280-6164

DOCUMENTI IAI 18 | 03 - MARCH 2018

Istituto Affari Internazionali (IAI)

Founded by Altiero Spinelli in 1965, IAI does research in the fields of foreign policy, political economy and international security. A non-profit organisation, IAI aims to further and disseminate knowledge through research studies, conferences and publications. To that end, it cooperates with other research institutes, universities and foundations in Italy and abroad and is a member of various international networks. More specifically, the main research sectors are: European institutions and policies; Italian foreign policy; trends in the global economy and internationalisation processes in Italy; the Mediterranean and the Middle East; defence economy and policy; and transatlantic relations. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*Affarinternazionali*), two book series (*Quaderni IAI* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via Angelo Brunetti, 9 - I-00186 Rome, Italy
T +39 06 3224360
F + 39 06 3224363
iai@iai.it
www.iai.it

Latest DOCUMENTI IAI

18 | 03	Cristian Barbieri, Jean-Pierre Darnis and Carolina Polito, *Non-proliferation Regime for Cyber Weapons. A Tentative Study*
18 | 02	Florent Marciacq and Tobias Flessenkemper, *The European Union and its Eastern Partners: Beyond the Limits of Current Approaches to Regional Cooperation*
18 | 01	Anja Palm, *Services: A Key Element in Upgrading the EU-Turkey Customs Union?*
17 | 21	Carolina Polito, Andrea Aversano Stabile e Elena Cesca, *Quale futuro per la cooperazione Nato-Ue?*
17 | 20	Anja Palm, *Women, Peace and Security in the Mediterranean*
17 | 19	Andrea Aversano Stabile, Alessandro Marrone e Carolina Polito, *Europa della difesa: quali prospettive?*
17 | 18	Andrea Dessì, *EU Aid and Development Planning in the Occupied West Bank*
17 | 17	Andrea Dessì, *Peace Economics: Opportunities and Options for a Post-Conflict Middle East*
17 | 16E	Alessandro R. Ungaro, Paola Sartori and Federico Palmieri, *Italian Defence Reform: Toward a New Logistics Support Model?*
17 | 16	Alessandro R. Ungaro, Paola Sartori e Federico Palmieri, *Riformare la Difesa italiana: verso un nuovo modello di supporto logistico?*