Eunomia. Rivista semestrale di Storia e Politica Internazionali
Eunomia VII n.s. (2018), n. 1, 157-178
e-ISSN 2280-8949
DOI 10.1285/i22808949a7n1p157
http://siba-ese.unisalento.it, © 2018 Università del Salento

BRUNO PIERRI

Cyber Security and Cyber Crime: A Comparative Study in a New "Cold War" Scenario[*]

Abstract: *This work has the purpose to highlight the different interpretation of cyber security between Euro-Atlantic partners and the Sino-Russian world. On grounds of this, we can realise how alternative their stance on the global scenario is. In fact, in the last years the NATO Alliance has been accusing Moscow of steadily violating international agreements, thus jeopardising regional stability and democratic processes through the collaboration with cyber criminals. On the other hand, the Russians and the Chinese have been cooperating on several questions, including control of the Web and contrast to terrorism and any kind of extremism in the cyber domain. According to such an approach, the Net is an extension of the physical territory of an independent State. Therefore, the Executive has the right to safeguard its sovereignty and protect the nation's ways of life and core values. This is why Russia has not signed the Budapest Convention of Cybercrime, which claims that a contracting Party may give access or receive stored computer data located elsewhere, without authorisation of another Party. In a few words, we can state that the Cold War has moved to the Internet.*

Keywords: Cyber threats; Cyber security; Neo-Cold War; East-West confrontation.

Introduction

Cyber threat is extremely complex, constantly evolving around transnational criminal organisations, and affecting cyber attacks, that is web activities carried out through a system of information instructions. Illicit activities in the virtual world are typically associated with the "Dark Web," a sub-set of the Internet where IP addresses of websites are concealed. Here, the sale of drugs, weapons, counterfeit documents and child pornography have literally become flourishing industries[1]. According to the latest Europol Internet Organised Crime Threat Assessment (IOCTA), in some EU countries police reports dealing with cyber crime have by now overcome those relating to traditional criminality. What is interesting in the IOCTA report is the width of cyber crime geographic distribution, allowing any sort of criminal organisation to exploit the Net all over the planet.

---

* *TA4eae*

[1] See A. GREENBERG, *Hacker Lexicon: What Is the Dark Web?*, in «Wired», November 19, 2014, in http://www.wired.com.

As concerns Africa, the most commonly reported threats seem to be social engineering attacks and cyber-facilitated frauds, due to the fact that this continent hosts nearly ten per cent of the world's Internet users, though almost one third of African countries enjoy less than one tenth of Internet penetration.[2] In North America, instead, despite an Internet penetration of over eighty-eight per cent, there is a smaller percentage of users than in Africa, that is only 8.6 per cent. Nevertheless, this part of the world is a key target for financially motivated cyber crime, in terms of frauds and data breaching, number of records stolen and average cost per breach, as well as being identified as a primary origin of children being featured in imagery abuse. As regards Asia, here there are over half of the world's web users, but despite this the continent is the focus for a disproportionately small percentage of cyber threats. Countries in Asia do however feature heavily as victims of cyber crime, and many of them, such as India, Taiwan, Malaysia, South Korea and Pakistan, also feature the highest rates of attacked computers. Concerning the EU, it is perhaps unsurprising that the majority of threats are identified as coming from within Europe, especially those dealing with social engineering, Internet-facilitated sexual offences against children, malware, and attacks on critical infrastructure. Eastern Europe, instead, is reported as a key source of ATM malware. Russia is also reportedly home to a number of advanced persistent threat attack groups.[3]

Aiming at bridging differences among EU countries and reaching a minimum security level for technology and digital services, the European Commission adopted its own cyber security strategy in 2013. Such a document highlighted five priorities, that is to say: a) achieving cyber resilience; b) drastically reducing cyber crime; c) developing

[2] In 2014, the African Union adopted the Convention on Cyber Security and Personal Data Protection, inviting all States to establish all appropriate measures aiming at cyber security governance and combating cyber crime. See *African Union Convention on Cyber Security and Personal Data Protection*, Adopted by the Twenty-Third Ordinary Session of the Assembly, Held in Malabo, Equatorial Guinea, 27 June 2014, in https://au.int; to make the implementation of the Convention easier, in 2017 the African Union Commission developed guidelines to put forward Internet security principles, tailoring everything to the African cyber security features, that is a shortage of skilled human resources, limited financial resources, limited levels of awareness of cyber security issues among stakeholders, and a general lack of awareness of the risks involved. See *Internet Infrastructure Security Guidelines for Africa: A Joint Initiative of the Internet Society and the Commission of the African Union*, May 30, 2017, in https://www.internetsociety.org.

[3] See EUROPOL, EUROPEAN CYBERCRIME CENTRE, *Internet Organised Crime Threat Assessment (IOCTA)* 2017, in www.europol.europa.eu.

cyber defence policy and capabilities; d) developing industrial and technological resources for cyber security; e) establishing a coherent international cyber space policy and promoting core EU values. In order to implement these policies, both public authorities and the private sector must develop capabilities and cooperate effectively through a cross-border dimension, also exploring possibilities on how the EU and NATO could complement their efforts. Finally, a critical point which has by now become a source of controversy with Russia and China was the paragraph stating that preserving open, free and secure cyber space would always be a global challenge. In light of this, the Commission undertook to seek to promote openness and freedom of the Internet, encourage efforts to develop norms of behaviour and apply existing international laws in cyber space, being always led by EU core values of human dignity, freedom, democracy, and respect for fundamental rights. Hence, the documents stated the necessity to provide analysis and intelligence, support investigations, facilitate cooperation, and create channels for information sharing among the competent authorities in the member States.[4] Within this frame, two years later the Commission highlighted the need for a strong EU response to terrorism. At the same time, serious and organised cross-border crime was finding new avenues to operate, such as trafficking in human beings, trade in firearms, drug smuggling, and financial, economic and environmental crime. In a few words, terrorism, organised crime and cyber crime were regarded as three core priorities to face. Moreover, several directives provided national legislation to prevent child sexual abuse online.[5] As an evidence of the collaboration between the European Union and the United States, on December 5, 2012, the Global Alliance Against Child Sexual Abuse Online was launched, aiming at raising standards worldwide and uniting efforts around the world to more effectively combat online sexual crimes against children. Gathering fifty-four countries, it is committed to pursue concrete actions in four key policy areas:

[4] See EUROPEAN COMMISSION, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, February 7, 2013, JOIN (2013) 1 final, in https://eeas.europa.eu.

[5] See EUROPEAN COMMISSION, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security*, Strasbourg, April 28, 2015 COM (2015) 185 final, in www.cepol.europa.eu.

1) identifying victims in order for them to receive the necessary assistance, support and protection; 2) investigating cases of child sexual abuse online; 3) increasing awareness among children, parents, educators and the community at large about the risks; 4) reducing the availability of child pornography online and re-victimization of children.[6]

As concerns the United Nations, in 1998 Russia introduced a draft resolution on the developments in the field of information and communication. Since then, every year the General Assembly has always approved a resolution on that question. Moreover, on Russian request a Group of Government Experts (GGE) coming from fifteen members was established, with the purpose to produce proposals on an international level. The aim of this process was to build cooperation for a peaceful, secure, resilient and open cyber environment by agreeing upon rules and principles of responsible behaviour and exchange of information. The GGE issued a consensus report in 2010, recommending a series of steps to reduce the risk of misperception resulting from web and information disruptions, but did not forward any binding agreements.[7] However, such a format is not without points of weakness, due first of all to the lack of binding Security Council Resolutions, and then to the different approach of China and Russia, on one hand, and the United States on the other hand. In a few words, there is no shared interpretation on how international law may be implemented on cyber space. In September 2012, the U.S. State Department took a public position on whether cyber activities could constitute a use of force under the U.N. Charter and customary international law. According to Harold Koh, Department of State legal advisor during the Obama Administration, cyber activities provoking death, injury, or significant destruction would likely be considered as a use of force. Koh focused his attention on the outcome of a cyber attack, rather than the means with which it would be carried out.[8] However, the United States recognizes that cyber attacks without kinetic effects are also an element of armed conflict under certain circumstances, such as an attack on information networks in the course of an on-

[6] See *We Protect Global Alliance to End Child Sexual Exploitation Online*, in https://ec.europa.eu.
[7] See UNITED NATIONS GENERAL ASSEMBLY, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, July 30, 2010, in www.un.org.
[8] See C.A. THEOHARY - J.W. ROLLINS, *Congressional Research Service Report - Cyberwarfare and Cyberterrorism: In Brief*, March 27, 2015, R 43955, in https://fas.org.

going armed conflict, which would imply retaliation with a proportional use of kinetic force[9]. On the other hand, Russia and China introduced a revision of the UN international code of conduct for information security, stressing the commitment for each State to respect the sovereignty, territorial integrity and political independence of all, as well as respect for human rights and the difference of history, culture, and social systems of any country. What the representative of the Euro-Asian members wanted to underline was the appeal not to use information technology to interfere in the international affairs of other States, or to undermine their political, economic, and social stability.[10]

1. *The Convention of Budapest: A Comparison with Chinese Criminal Law*

The so-called Budapest Convention on Cybercrime, drafted by the Council of Europe in 2001, is the first international document aiming at harmonising legislation on criminal activities online, being also open for ratification to non members of the Council of Europe. The Convention broadly attempts to cover crimes of illegal access, interference and interception of data and system networks, and the criminal misuse of devices, as well as computer-related fraud, production, distribution and transmission of child pornography and copyright offences. Aiming at a comparative study with non-Western powers' initiatives, what is interesting to highlight is what is stated in articles nine, twenty-three, and thirty-two of the Convention. As concerns article nine, this is relating to child pornography offences, stating that each Party shall adopt such legislative and other measures on the following conduct: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer

[9] See *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, May 2011, in https://obamawhitehouse.archives.gov.
[10] See UNITED NATIONS 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*, Sixty-ninth Session, Agenda Item 91, *Developments in the Field of Information and Telecommunications in the Context of International Security*, January 13, 2015, Distr.: General, A/69/723, in http://repository.un.org.

system for oneself or for another person; e) possessing child pornography in a computer system or on a computer-data storage medium.[11]

On the other hand, the relevant provisions in Chinese Criminal Law are regulated in Articles 363-367, defining the crime of producing, duplicating, publishing, selling or disseminating pornographic materials for the purpose of profit, and the crime of disseminating pornographic materials.[12] According to Pi Yong, Professor of Law at Wuham University, People's Republic of China, the offences related to child pornography of the Convention of Budapest do have differences with the same crime in Chinese Criminal Law.[13] First of all, the criminal object of the Convention are child pornography materials, so that the legislative purposes is to protect children against being used in sexual activities; the criminal object of the Chinese Criminal Law are pornography materials, including adult pornography materials as well as child pornography materials, so that the legislative purpose is to protect a good social environment. Moreover, while the Convention states that criminal conduct is producing, offering or making available, distributing or transmitting, procuring or possessing child pornography through a computer system,[14] the Chinese code affirms that what is punishable is producing, duplicating, publishing, selling or disseminating pornographic materials. In addition to that, paragraph 1 of Article 363 requires the purpose of making profit to convict the crime, so that the condition to establish this crime is stricter; the provision in the Convention only requires the purpose of distributing child pornography materials through a computer system to convict crime, while paragraph 1 of Article 364 requires that the circumstances of disseminating pornography materials be serious in order to convict the crime. From the comparison above, the outcome is that China lacks legislation against child pornography crime, as the Chinese Criminal Law does not differentiate between child pornog-

[11] See COUNCIL OF EUROPE, European Treaty Series No. 185, *Convention on Cybercrime*, Budapest, 23 November 2001, in https://rm.coe.int.
[12] See NATIONAL PEOPLE'S CONGRESS, Order of the President of the People's Republic of China No. 83, *Criminal Law of the People's Republic of China*, March 14, 1997, in www.fmprc.gov.
[13] See PI YONG, *Comparative Research on "Convention on Cybercrime" and Chinese Relevant Legislation*, in https://www.coe.int.
[14] See COUNCIL OF EUROPE, European Treaty Series No. 185, *Convention on Cybercrime*, cit.

raphy crime and other crimes of producing, selling and disseminating pornography materials.[15]

Going back to the Convention of Budapest, the principle relating to international cooperation is stated in article 23, calling the Parties to collaborate to the widest extent, to the purpose of investigation and collection of evidence of any electronic form of criminal offence.[16] However, the reason why the Russian Federation is the only member of the Council of Europe which has not signed the Convention on cyber crime may be searched in the provisions of Article 32, saying that a Party may access open source computer data, regardless of where the data are geographically located, as well as giving access or receiving stored computer data located elsewhere, without authorisation of another Party. In particular, Moscow finds this provision to be an intolerable infringement of State sovereignty. A key divergence with the Western approach to cyber security is the Russian perception of cyber space, which must be considered as an extension of the physical territory of an independent State, thus subject to government jurisdiction. Therefore, each country should have the right to control the Web the way they like. On the contrary, the Organisation for Economic Cooperation and Development (OECD) recommendations include free flow of information and knowledge, freedom of expression, association and assembly, protection of individual liberties,[17] as also said by the British Foreign Secretary, William Hague, at the London International Conference on Cyberspace on 1-2 November 2011.[18]

Nevertheless, a pivotal difference was expressed at the same conference by the Russian Minister Shchegolev, who underlined several limits to the principle of free flow of information, as this should be subject both to national legislation, and to counterterrorism considerations, thus giving priority to security interests.[19] The question of

[15] See PI YONG, *Comparative Research*, cit.
[16] See COUNCIL OF EUROPE, European Treaty Series No. 185, *Convention on Cybercrime*, cit.
[17] See *OECD Council Recommendation on Principles for Internet Policy Making*, December 13, 2011, in www.oecd.org.
[18] See W. HAGUE, *London Conference on Cyberspace: Chair's Statement*, November 2, 2011, in www.gov.uk.
[19] See K. GILES, *Russia's Public Stance on Cyberspace Issues*, in C. CZOSSECK - R. OTTIS - K. ZIOLKOWSKI, eds., *2012 4th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallin, 2012, p. 65.

Internet sovereignty is another big source of disagreement. As a matter of fact, Russia agrees with China on the idea of national control of all Internet resources that lie within a State's physical border. This is in direct opposition to the approach of the United States, as expressed by Secretary of State Hillary Clinton in December 2011, when she clearly said that countries like Russia wished to empower each individual government to make their own rules for the Internet, thus undermining human rights and the free flow of information. The real intention behind such an approach, the Secretary stated, was to create national barriers in cyber space, which was exactly the opposite of Internet freedom.[20] Another pivotal field of divergence are the concept of terrorism, with a particular focus on what constitutes cyber terrorism, and the issue of access to a foreign State's information space, which stresses the dissent towards Article 32 of the Council of Europe Convention on Cybercrime. The statement "without the authorisation of another Party" for the Russians is an intolerable breach in the principle of sovereignty. Russian concerns are illustrated through a report in the official government newspaper which highlighted the «[. ..] dubious provision for foreign special services to invade our cyber space and carry out their special operations without notifying our intelligence services».[21]

If we remember that a year before the two conferences of London and The Hague the Chinese government had already published a White Paper on the use of the Net, there is nothing to be surprised if Russia has decided to co-operate with China on the question of cyber defence and cyber sovereignty. As concerns this, the White Paper "The Internet in China", published on December 8, 2010, gives us a clear explanation of how different the Oriental conception of the Net is, compared with the principles claimed by Western powers. The basic goals of China's Internet administration, it is stated, are to promote general and hassle-free web accessibility, regulate the order of Internet information transmission, and create a market environment for fair competition. Apart from this, we can read that the government has the duty to curb the effects of illegal information on

[20] See H. CLINTON, *Remarks by Hillary Rodham Clinton at Conference on Internet Freedom, The Hague, Netherlands*, December 8, 2011, in www.youtube.com, accessed on June 10, 2018.
[21] GILES, *Russia's Public Stance on Cyberspace Issues*, cit., p. 67.

State security, public interests and minors.[22] Therefore, the Administration clearly prohibits the spread of information with contents subverting State power, undermining national unity, inciting ethnic hatred and secession, advocating heresy, pornography, violence, terror, thus setting up Internet security management systems with the purpose to prevent all types of illegal information and strengthen legal and ethical education.

A pivotal paragraph is the one dealing with Internet security protection, regarded as an indispensable requirement for State security and public interest. The statement according to which within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty, thus respecting and protecting the cyber sovereignty of China, is what prevents Beijing from signing the Budapest Convention and what separates the Asian power from the way the West interprets freedom of access to the Net. On the question of secure information flow, despite the assertion that the Chinese government attaches great importance to protecting the safe flow of Internet information, at the same time any kind of content interpreted as harmful to Chinese sovereignty and State principles is strictly forbidden. The territorial unity of the nation, as well as the political supremacy of the Communist Party, or policies such as the so-called socialist market economy, but also religious and ethnic questions, must not be jeopardised by online dissent. Hence, all Chinese citizens, foreign citizens, and other organisations within the territory of China must obey the provisions forbidding production, duplication, or dissemination of information which may: a) endanger State security, divulge State secrets, subvert State power and jeopardise national unification; b) damage State honour and interests; c) instigate ethnic hatred or discrimination and jeopardise ethnic unity; d) harm State religious policy, propagating heretical or superstitious ideas; e) spread rumours disrupting social order and stability; f) disseminate obscenity, pornography, gambling, violence, brutality and terror.[23] Such a policy was confirmed a few years later, at the BRICS Summit in Brazil in July 2014, when Chinese President Xi Jinping called for respect of a

[22] See THE INFORMATION OFFICE OF THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA, *White Paper - The Internet in China*, June 8, 2010, in www.gov.cn.
[23] See *ibid*.

country's cyber space sovereignty, claiming the right for every country to preserve its own information security.[24]

2. *NATO on cyber defence*

By reading the documents issued by the North Atlantic Treaty Organisation on cyber space, it is quite easy to realise how alternative a stance the West takes. Actually, what is stated in NATO papers and declarations is a plea to collaboration with EU partners on a broad variety of matters, such as cyber defence, the proliferation of weapons of mass destruction, counter-terrorism, energy security, and maritime security. On the other hand Russia, despite official statements on the need of a joint effort to preserve the Web from cyber crime, is once again seen as the main representative of a completely different scenario, if not as an enemy trying to influence the political life of Western countries. As an evidence of this, the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales issued a common declaration about the policies to pursue on several world challenges. What is remarkable is that the Alliance recognised that international law and the UN Charter apply also in cyber space, affirming as well that cyber defence had become part of the Organisation's core task of collective defence, implying, on a case-by-case basis, the decision to invoke Article 5.[25]

As an implementation of such a statement, two years later the leadership of the European Union and NATO, that is to say Donald Tusk, President of the European Council, Jean-Claude Juncker, President of the European Commission, and Jens Stoltenberg, Secretary General of the North Atlantic Treaty Organisation, released a joint declaration on the NATO-EU strategic partnership, underlining the need to boost the mutual ability to counter hybrid threats, through timely information and intelligence sharing.[26] In order to foster research and technology in this field, the EU Computer Emer-

[24] See W. JIAO - Z. SHENGNAN, *Xi: Respect Cyber Sovereignty*, July 17, 2014, in http://usa.chinadaily.com.cn.
[25] See *Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales*, September 5, 2014, in www.nato.int.
[26] See EUROPEAN COMMISSION, *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, July 8, 2016, in http://europa.eu.

gency Response Team (CERT-EU)[27] and the NATO Computer Incident Response Capability (NCIRC)[28] were supposed to jointly develop their ability to innovate and cooperate with private industry.[29] As we can see, in the last few years the main European and Atlantic organisations have set up a common system to respond to cyber attacks and hybrid threats, which are now perceived as likewise dangerous as ballistic missile attacks from outside the Euro-Atlantic area. What may strike our attention most in these documents, however, is the way this updated collaboration seems to pursue the task to isolate Russia from the international forum, as a response to what is regarded as Moscow's cyber offensive against the West.

As a matter of fact, the Warsaw Summit of the North Atlantic Council of 8-9 July 2016 represents a watershed in the most recent relations between the West and the non Euro-Atlantic world, in terms of strictness of positions on global security and as regards the sharpness of the words chosen in the following communiqué, especially towards what was by then openly perceived as the Russian threat to world peace and stability. The document deals with cyber space in paragraphs 70 to 72, stating that the Web is recognised as a domain of operations in which NATO must defend itself in accordance with international law. All this must be pursued through close bilateral and multilateral cyber defence cooperation, especially by deepening collaboration with the EU. An important passage is the one relating to the possibility to invoke collective defence.[30] Apart from such a generic reference to cyber defence, the language becomes much sharper and more direct when Russia is involved, complaining for example that for the last two decades NATO has tried in any possible way to build a partnership with Russia, whose re-

[27] The Computer Emergency Response Team is composed of IT security experts from the main EU Institutions, with the aim to cooperate with other CERTs in the member States and with specialised IT security companies in order to respond to information security incidents and cyber threats.

[28] The NATO Communications and Information Agency (NCI Agency) Cyber Security (CS) Service Line (SL) is responsible for planning and executing all life cycle management activities for cyber security. Cyber Security incorporates the NATO Computer Incident Response Capability (NCIRC) Technical Centre, providing specialist services to prevent, detect, respond to and recover from cyber security incidents.

[29] See NORTH ATLANTIC TREATY ORGANIZATION, *Statement on the Implementation of the Joint Declaration Signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, December 6, 2016, in www.nato.int.

[30] See NORTH ATLANTIC TREATY ORGANIZATION, *Warsaw Summit Communiqué, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw*, July 8-9, 2016, in www.nato.int.

cent activities and policies have reduced stability, increased unpredictability, and changed the security environment. Such a statement is followed by serious allegations for Moscow to have breached the values, principles and commitments outlined in previous agreements, such as the 1997 Basic Document of the Euro-Atlantic Partnership Council,[31] and the 1997 NATO-Russia Founding Act.[32] Therefore, Russia is accused of destabilising actions, including the ongoing illegal and illegitimate annexation of Crimea, the violation of sovereign borders by force, the deliberate destabilisation of Eastern Ukraine, and repeated violations of NATO Allied airspace.[33] What is even worse is the pessimistic mood towards future NATO-Russian relations, especially after the annexation of Crimea in 2014. Despite the strategic value of a partnership between the Atlantic Alliance and Russia, the papers clearly state that at the moment the conditions for such a cooperation do not exist, as long as Moscow does not show compliance with international law and its own international obligations and responsibilities. What Euro-Atlantic Heads of State and Government blame Russia for, is the violation of the points expressed in the 2002 Rome Summit NATO-Russia Council, in particular as concerns the mutual determination to build together a lasting and inclusive peace under the obligations provided in the UN Charter, the provisions and principles contained in the Helsinki Final Act and the OSCE Charter for European Security.[34]

Trying to read this document from a Russian point of view, what might be worrying are probably paragraphs 40 and 41, which are not hard to interpret as a sort of encirclement from the West. As an evidence of that, through the Warsaw Declaration NATO decided to establish an enhanced forward presence in Estonia, Latvia, Lithuania and Poland, with multinational forces provided by framework nations and other contributing allies to unambiguously demonstrate solidarity, determination, and ability to act by triggering an immediate response to any aggression. Furthermore, the Alliance accepted the

[31] See NORTH ATLANTIC TREATY ORGANIZATION, *Basic Document of the Euro-Atlantic Partnership Council*, May 30, 1997, in www.nato.int.
[32] See *Founding Act on Mutual Relations, Cooperation and Security between NATO and the Russian Federation Signed in Paris, France*, May 27, 1997, in www.nato.int.
[33] See NORTH ATLANTIC TREATY ORGANIZATION, *Warsaw Summit Communiqué*, cit.
[34] See NATO-RUSSIA COUNCIL, Rome Summit 2002, *Declaration by Heads of State and Government of NATO Member States and the Russian Federation*, NATO Office of Information and Press, in www.nato.int.

Rumanian initiative to establish a multinational framework brigade to help improve integrated training around the Black Sea region, also increasing ballistic missile defence effectiveness and extending the defence building initiative to Moldova.[35] The strategy of NATO on cyber security is based on the two core principles of collective defence and resilience, thus taking care of improving the means for sharing information and promote a deeper knowledge of existing threats, also providing the integration of cyber defence into operational planning and assistance in case of cyber attack.[36] However, the allies are far from adopting a common view on the conditions in which the use of force may apply in case of a malicious act in cyber space.[37]

According to the U.S. Center for Cyber and Homeland Security, there are four main threats in the cyber domain: a) nation-States, as every country with a modern military and intelligence service has also network attack capability; b) foreign terrorist organisations, which have not fully developed a cyber-attack capability yet; c) criminal organisations driven by profit motivations, some of which are increasingly working for States such as Russia; d) hactivists, aiming at bringing attention to their cause.[38] The kind of danger perceived as most threatening to U.S. security are thought to be those coming from nation-States and their proxies, in particular China and Russia. Actually, the former is said to possess sophisticated cyber capabilities and reports of the Office of the U.S. National Counterintelligence Executive have classified Chinese cyber activities as

[35] See NORTH ATLANTIC TREATY ORGANIZATION, *Warsaw Summit Communiqué*, cit.

[36] NATO's legal framework is based on the Tallinn Manual on the International Law Applicable to Cyber Warfare, previously published in 2013 and then updated four years later. The documents affirm that it is up to international law to regulate the actions of States into cyberspace. In particular, the new version offers a set of guidelines on rules of engagement, countermeasures, retaliation operations, and other forms of response in case of cyber aggression. See M.N. SCHMITT, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York, Cambridge University Press, 2013; M.N. SCHMITT, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, New York, Cambridge University Press, 2017.

[37] See G. PIERINI, *Cyber Security Meets Diplomacy: The EU-NATO Cooperation and the Italian Case*, LUISS Guido Carli, Department of Political Science Master's Degree in International Relations – Global Studies, Academic Year 2016/2017, pp. 45-49, in https://tesi.luiss.it.

[38] See *Emerging Cyber Threats to the United States*, Testimony of Frank J. Cilluffo Director, Center for Cyber & Homeland Security Before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, February 25, 2016, Center for Cyber & Homeland Security, The George Washington University, in https://docs.house.gov.

rising to the level of strategic threat to the U.S. national interest.[39] As a matter of fact, the People's Republic of China is accused of amassing data and secrets able to further support the country's economic growth, as well as scientific, technological, and military capacities. As concerns the Russian Federation, its cyber capabilities are even more sophisticated, aiming at collecting economic information and technology to support Russia's economic development and security. This is why the former communist superpower has been registered as a long-term strategic threat to the United States, especially after signing a cyber security agreement with China, pledging both parties not to hack each other and to share information and technology.[40] The Americans are worried about a toxic blend of crime, business, and politics in a sort of convergence between the Russian intelligence community and cyber criminals, while relations between Russia and the West are deteriorating more and more. As a clear evidence of this collaboration with cyber criminals, the Americans quote a public notice, issued by the Russian Foreign Ministry, advising citizens to refrain from travelling abroad, especially to countries that have signed agreements with the U.S. on mutual extradition.[41] To even better understand how wrecked the relations between the United States and Russia are, suffice it to quote what James R. Clapper, former Director of National Intelligence, reported before the Senate in 2016, when he stated that Russia was «[...] assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected».[42]

The 2018 National Intelligence Worldwide Threat Assessment, instead, warns about a growing risk for some adversaries to conduct cyber attacks short of war against the U.S in a crisis. In particular, Russia and China are said to be posing the greatest cyber threat to the United States for the next years. In light of such a statement, these States are accused to be using cyber operations as a low-cost tool of statecraft to achieve strategic objectives. As concerns Russia, the American intelligence expects Moscow to

[39] See *Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011: Foreign Spies Stealing Us Economic Secrets in Cyberspace*, October 2011, in http://www.ncix.gov.
[40] See *Emerging Cyber Threats to the United States*.
[41] See K. POULSEN, *Russia Issues International Travel Advisory to its Hackers*, in «Wired», September 3, 2013, in www.wired.com.
[42] J.R. CLAPPER, *Worldwide Threat Assessment of the US Intelligence Community, Statement for the Record before the U.S. Senate, Armed Services Committee*, February 9, 2016, in www.dni.gov.

conduct bolder and more disruptive cyber operations, probing U.S. and allied critical infrastructures, aiming at disseminating false information via Russian State-controlled media to encourage anti-American political views, thus seeking to reduce trust and confidence in democratic processes, degrade democratization efforts, and undermine the effort to bring Ukraine and other former Soviet republics into European institutions. On the other hand, China is suspected to be continuing to use cyber espionage and bolster cyber attack capabilities to support national security priorities. Finally, Washington experts predict the line between criminal and nation-State activity to become increasingly blurred as governments view cyber criminal tools as a relatively inexpensive and deniable means to enable their operations.[43]

3. *The Sino-Russian co-operation on cyber space*

As a response to the Western approach to cyber security and information sharing, the former enemies of the communist world are tightening their relations more and more, thus moulding an opposite vision of information security matters. Moscow's and Beijing's policies have converged so much, that in 2015 the two giants of the East reached an agreement on cooperation in ensuring international security in the cyber domain. If we read carefully the text of this treaty, we can easily realise how Russia and China are always concerned about threats related to the use of such technology with the purpose to undermine the sovereignty and security of States and interference in their internal affairs. Article two quotes the threat of using the Web for terrorist purposes, thus following the policy pursued by the Shanghai Cooperation Organisation since its foundation in 2001.[44] On grounds of this, the agreement authorises representatives and the competent authorities of the two States to cooperate in ensuring international information security

[43] See D.R. COATS, *Worldwide Threat Assessment of the US Intelligence Community, Statement for the Record*, February 13, 2018, in www.dni.gov.
[44] See *Declaration on the Establishment of the Shanghai Cooperation Organization*, in www.gsdrc.org.

to investigate cases involving the use of information and communication technologies for terrorist and criminal purposes.[45]

The following year, the Chinese government issued its national cyber space security strategy, highlighting that national sovereignty had extended and stretched into cyber space. According to this statement, the Executive's main concern is granting its stability, seen as a precondition for national development and the happiness of the people. Hence, what is to avoid is the use of networks to interfere in the internal political affairs of other countries, inciting social unrest. An important difference with the Western approach is the focus on the moral sphere and life style with the purpose to protect the Socialist code of values. In light of this, the government has the duty to prevent online rumours, degenerate culture, obscenity, violence, superstition and any harmful information from corroding the physical and mental health of minors, influencing social harmony and stability, and misleading value orientations.[46] A few months previously, in March 2016 the Chinese government had launched the national innovation portion of its 13th Five-Year Plan, including its commitment to "Internet plus", designed to drive economic growth and foster new industries by integrating web technology with Chinese business and manufacturing. Shortly afterwards, President Xi Jinping chaired a cyber security and information forum, during which he emphasized the value of the Internet as a tool to improve the flow of information, technology, capital, and talent, as well as goods and services.[47] The Chinese national strategy is based on a series of principles, among which there is first of all respect and protection of sovereignty in the web domain, with the consequent right of any country to independently choose their network management method, thus formulating laws and regulations on the basis of their national circumstances to protect information systems. What strikes our attention is the steadfast position on the need to keep independence on cyber security policy, with the relating appeal that no country should engage in cyber hegemonies and use the network

[45] See Government of the Russian Federation Order No. 788-P, *Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in Ensuring International Information Security*, April 30, 2015, in www.csis.org.

[46] See *National Cyberspace Security Strategy*, December 27, 2016, in https://chinacopyrightandmedia.wordpress.com.

[47] See BY JING DE JONG-CHEN, *China's Evolving Cybersecurity and Cyber Development Strategy*, March 29, 2017, in «The National Bureau of Asian Research», in www.nbr.org.

to interfere in the domestic affairs of other countries. All countries, instead, should persist in mutual respect and seek common ground while accepting differences, without trying to control other countries' networks and information systems, or collect and steal data from other countries.[48]

As regards the tasks pursued by the People's Republic of China, these may be summarised as follows: a) defending sovereignty in cyberspace, thus opposing all actions to subvert the country's national regime; b) safeguarding national security, thus preventing any act of using the network to engage in treason, separatism, incite rebellion or subversion, or steal or leak State secrets, also by punishing foreign powers promoting separatist activities; c) protecting critical information facilities, thus controlling also basic information networks providing public telecommunications, as well as important information systems in fields such as energy, finance, education, scientific research; d) strengthening the construction of online culture to foster and practice the Socialist core value view; e) opposing cyber terrorism and crime, including dissemination of obscenity and sex; f) enhancing cyber space protection capabilities to resist cyber intrusions.[49] In a few words, such a piece of legislation outlines responsibilities for service providers to address content censorship, enforce real-name registration for Internet services, give mandatory assistance to law enforcement, and require data residence of personal and important data associated with critical infrastructure. Apart from this, organisations with information or systems not located in the Asian country must also review their technology architecture and business processes if they want to reduce the risk of being prosecuted.[50]

The other actor of what we may call "Web Cold War" is Russia, which views cyber and hybrid war as strategic tools to respond to what it regards as long-term Western support for regime change stretching back to the disintegration of the USSR and the so-called coloured revolutions in the Balkans, Eastern Europe and Eurasia. Such a belief is testified by President Putin's words, accusing the West of aiming at finishing Russia off, after the Soviet Union had collapsed. Therefore, colour revolutions are seen as the

[48] See *National Cyberspace Security Strategy*, cit.
[49] See *ibid*.
[50] See R. HÄNI, *China's Cyber Security Law – Technical Implications*, December 2017, in https://news.pwc.ch.

equivalent of Western soft power aiming at the hard expansion of NATO and the EU. Hence, when the EU-Eastern Partnership was launched in 2009 for post-Soviet countries such as Ukraine and Georgia, Russia launched a competing Customs Union that became the Eurasian Economic Union in 2015, with Armenia being pressured to withdraw from the former in favour of the latter. In April 2008, speaking to the NATO-Russia Council at the Bucharest NATO summit, Putin described Ukraine as an "artificial" country and questioned Kiev's right to control its Russian speaking Eastern and Southern regions, thus claiming as a legitimate policy Russia's right to intervene in its neighbours to "protect" Russian speakers.[51] Actually, the cyber domain has provoked a shift in Russian doctrine, as cyber has been turned into a means to obtain asymmetric advantage. The origins of such a new approach may be dated back to 2013, when the then Chief of the General Staff, Valeri Gerasimov, wrote an article and delivered a speech which is by now commonly referred to as the "Gerasimov Doctrine". Gerasimov stated that methods of conducting military operations that cannot be considered purely military have emerged. On grounds of this, he added that the role of non-military means in achieving political and strategic goals had grown, and that in modern reality Russia must look to non-military instruments.[52] As of December 2016 and amid Western and former Soviet-sphere countries accusing Moscow of waging informational warfare campaigns, the Kremlin released its new Information and Security Doctrine, highlighting the need to counter propaganda, informational-psychological influence by foreign intelligence services and recruitment efforts by terrorist organisations, and to secure computers from cyber espionage and cyber crime aimed at disrupting the historical foundations and patriotic traditions associated with the defence of Russia.[53] According to Stephen R. Covington, Russia's assessment of technological inferiority has reinforced perceptions of strategic vulnerability in traditional Russian culture, impacting its approach to war and the need to invest in information and cyber capabilities. Technological vulnerability is

[51] See T. KUZIO, *Why Vladimir Putin is Angry with the West: Understanding the Drivers of Russia's Information, Cyber and Hybrid War*, Federal Academy for Security Policy, Security Policy Working Paper, No. 7/2017, in www.baks.bund.de.
[52] See *The "Gerasimov Doctrine" and Russian Non-Linear War*, in «In Moscow's Shadows», July 6, 2014, in https://inmoscowsshadows.wordpress.com.
[53] See *A Shift in Russian Doctrine*, International Centre for Defence and Security Paper Issue, August 11, 2017, in https://icds.ee.

seen first and foremost as the inability to match the West's revolutionary leaps in technological innovation for weapons system development. Thus, Russia requires a different approach towards this perceived Western advantage.[54]

Having said this, there is no need to be surprised if President Putin delivered the basic principles of foreign policy of the Russian Federation just a few months after the NATO Warsaw Declaration and barely a month before the Chinese published their own concept of national cyber security. Concerning the collaboration with Beijing, the words used by the Russians are practically the same as those we can read in Chinese papers. For example, point 28 of the Foreign Policy Concept of the Russian Federation states as follows: «Russia takes necessary measures to ensure national and international cyber security, counter threats to State, economic and social security emanating from cyber space, combat terrorism and other criminal threats involving the use of information and communication technology; deters their use for military-political aims that run counter to international law, including actions aimed at interfering in the domestic affairs of States or posing a threat to international peace, security and stability [...]».[55] What is even more interesting to highlight is probably the paragraph on the relations with NATO, which replies to all Western allegations. Moscow accuses the Atlantic Alliance and the EU to pursue geopolitical expansion, along with their refusal to implement the creation of a common European security and cooperation framework. The Russian Federation maintains its negative perspective towards NATO'S military infrastructure approaching Russian borders, and its growing military activity in regions neighbouring Russia, viewing them as a violation of the principle of equal and indivisible security. Such a stance, according to the Kremlin, is the reason why in the last twenty-five years there has been a serious crisis in the relations between Russia and the West, thus preventing cooperation against global challenges and threats.[56] On the contrary, Russia claims equitable

[54] See S.R. COVINGTON, *The Culture of Strategic Thought behind Russia's Modern Approaches to Warfare*, Belfer Center for Science and International Affairs Paper, Harvard Kennedy School, Cambridge, MA, October 2016, p. 22.
[55] *Foreign Policy Concept of the Russian Federation*, November 30, 2016, in www.mid.ru.
[56] The U.S. 2016 Presidential Policy Directive orders Federal agencies to undertake three concurrent lines of effort: threat response, asset response, and intelligence support and related activities. Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; asset response activities include furnishing technical assistance to affected enti-

partnership with the Western alliance, on grounds of the commitment undertaken within the Russia-NATO Council to refrain from seeking to ensure one's security at the expense of the security of other States. As concerns the relations with the former rival of the Cold War, point 72 reminds the goal to build mutually beneficial relations with the United States of America, taking into consideration that such a dialogue could positively develop only when conducted on equal footing and non-interference in each other's domestic affairs.[57] On the other hand, the alliance with China is strengthened and supposed to continue on a basis of a comprehensive, equal partnership and strategic cooperation, thus being turned into one of the core elements of regional and global stability.

Conclusions

In 2017, important decisions were reached during the G7 meetings. First of all, the risk of escalation and retaliation in cyber space is not to underestimate, including massive denial-of-service attacks, damage to critical infrastructure impairing the use and operations providing services to the public, with a possible destabilizing effect on international peace and security and interference in democratic political processes. According to the Lucca Declaration on responsible behaviour in cyber space, the G7 group is committed to promoting a strategic framework for conflict prevention, cooperation and stability, recognising the applicability of existing international law to the world wide web. Under some circumstances, the foreign ministers of the seven world most industrialised countries reminded that cyber activities could amount to the use of force or an armed attack, thus implying the right for victim States to exercise their faculty of individual or collective self-defence.[58] To increase predictability and stability in cyber space, all States are invited to publicly explain their views on how existing international

ties to protect their assets; intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence, with the ability to degrade or mitigate adversary threat capabilities. See *Presidential Policy Directive: United States Cyber Incident Coordination*, July 26, 2016, in https://obamawhitehouse.archives.gov.

[57] See *Foreign Policy Concept of the Russian Federation*, cit.

[58] See *G7 Declaration on Responsible States Behavior in Cyberspace*, Lucca, April 11, 2017, in www.mofa.go.jp.

law applies to governmental activities in the cyber domain, thus laying the basis of the wide contrast between the Western interpretation of cyber security and government use of the Web on one hand, and the Sino-Russian vision of cyber space on the other. The following month, through the Taormina Declaration on the struggle against terrorism and violent extremism, the G7 leaders undertook to shift the challenge to a higher level, with a particular focus on the cyber dimension of such a threat, urging private industry and service providers to develop new technologies monitoring violent behaviour online. All this, the document states, must be carried out respecting the principles of democracy, safeguarding of human rights and the rule of law.[59]

On the other hand, the relations between the European Union and the Russian Federation have become rather unstable, as shown in an in-depth analysis on Russian diplomacy and foreign policy issued by the EU Directorate General for External Policies in 2017. According to such a paper, the idea that Russia should be recognised as a great power has driven Moscow's posture on the world stage for several centuries. Actually, the Russians are accused of feeling nostalgia of the Cold War era, when they stood as one of the two superpowers. Among other things, the Kremlin's new security strategy claims to increase the Russian role in the emerging polycentric world, on grounds of a global dangerous and volatile scenario, characterised by stiff competition for resources, control of markets and transport routes, as well as political influence amongst major powers. Therefore, Russia has not forgotten the inclination to surround itself with buffer zones as a protection from invasions and external instabilities, thus trying to control neighbouring nations, through for example a Eurasian integration process with countries once belonging to the Soviet Union. As a consequence of that, Russia views Western States and organisations as obstacles to the realisation of its ambitions.[60] What seems more worrying for Brussels is the verification that seeking a strategic partnership with the European Union has become less prominent in Russia's general strategy, for Moscow increasingly perceives the EU as strategically less and less relevant. Hence, a part-

[59] See *G7 Taormina Statement on the Fight Against Terrorism and Violent Extremism*, May 2017, in www.g7italy.it.
[60] See POLICY DEPARTMENT, DIRECTORATE-GENERAL FOR EXTERNAL POLICIES, *Russia's National Security Strategy and Military Doctrine and Their Implications for the EU*, January 2017, in www.europarl.europa.eu.

nership with the EU appears less valuable than strategic convergence with China and other major rising powers. In addition, Russia sees the EU as a kind of a strategic continuation of the United States and NATO. This perception has been compounded by the fact that EU countries that are also NATO members have repeatedly opposed Russia's critical positions on the Atlantic Alliance's policy.[61]

In light of all this, cooperation prospects between Russian and Western Europe appear quite grim and will remain so should the current political circumstances persist in the future, despite economic and energy agreements. In addition, we can say that the old Cold War has moved to the Web, as in the last years the United States has been pursuing a policy of neo-containment, with an approach to former Soviet satellites which is regarded as extremely harmful to Russian national interests. We know that threats to Russian security have always come from the West, from the Swedes in the XVIII century, to the Germans in both world wars, and NATO missiles in Western Europe. Therefore, it is easy to realise that Moscow simply does not trust the West as concerns information sharing and cyber security principles, seeing what the Atlantic Alliance and the European Union condemn as a way to safeguard its right to play a global role on the international chess board. In conclusion, the Kremlin perceives the dialogue with the Euro-Atlantic area as a cooperation between equal but different actors, aiming at carving out for itself a leading role in the Euro-Asian region in alliance with the Chinese giant, with which being able to extend their area of influence not only in Asia and the former Soviet republics, but also in Africa and Latin America, on grounds of national security interests and foreign policy aims difficult to conciliate with those of the West.

[61] See A. ZOLOTOV, *Detachment rather than Estrangement Will Save Russia-European Relations*, November 2, 2016, in www.russia-direct.org.