AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare ISSN 2038-3711

Cyber-Security and Nations: How Italy could react

di Andrea Chiappetta[*]

8 giugno 2020

Summary: 1. Introduction. – 2. New International Cyber Convention. – 3. om Diverging Views to Common Interests. – 4. Next Steps. – 5. Pledge by 27 nations on cyber-security. – 6. Norm, ICTs, and global security and peace. - 7.The United Nations, ICTs, and International Security and Peace. - 8.The origin of the norm-shaping efforts of ICT in the framework of international peace and security. - 9. State of the art in Italy.

1. Introduction

There has been an increase in issues that are related to cyber-security, and this has led to the adoption of many measures at both the national and regional levels, in particular during the COVID 19 pandemic showed how many critical infrastructures were attacked (ex: hospitals). However, actions at the United Nations have been relatively slow. Since the introduction of the draft resolution by the Russian Federation, most part activities have been impended since there have been fundamental differences between the United States and the Federation of Russia. However, in 2010, the United States acted as a co-sponsor to this resolution for the first time, and since then, The U.N. has been experiencing discernable momentum on issues relating to the cyber-security. This momentum has been increased by some cyber-attacks in Estonia, Georgia and Iran in 2007, 2008 and 2010 respectively (Buchanan, 2016)[1].

Additionally, there have been revelations about nations being spied by other nations and the vice versa. The U.N. Security Council has witnessed the cyber-security issues in the context of terrorism, the social and economic council as well as other organs and agencies that are affiliated with the U.N. As a way of enabling norm development and further integrated concerted action, there must be an improvement in communication and dialogue between various bodies, organs and groups of the United Nations.

[*] CEO @ Aspisec, PhD Università degli Studi di Roma Tor Vergata.

[1] Buchanan, B. (2016). *The cybersecurity dilemma: hacking, trust, and fear between nations*. Oxford University Press.

Disruptions of information infrastructure at the regional and global levels are where the far-reaching and most consequences will come from. Regional and global interruptions might not be the goal of the actor. However, this is likely to happen as an intended consequence whereby cyber-attacks are used as part of the conflict and possibly done together with physical attack forms. For example, let us say that there are two rival powers in the region, and each of them is intending to weaken the other nation (Tagert, 2010)[2]. Country A could launch a significant volume attack, and this will be followed by physical attacks that target the information infrastructure such as fiber-optic cables and routers. This attack aims to disrupt the economic activities of country B. There might be other countries that depend on country B to provide financial services. Since the economy of country B has been severely affected, the country depending on country B will be affected, leading to a severe drop in the gross domestic product in the other countries in the region. As unintended consequences, there could be overburdening of the ICT sector capacities due to the rerouting of the data traffic through satellites, and this could lead to countries experiencing different domino effects (Swaine, 2013)[3].

There would also be a technological failure in case of an interruption of the global ICT sector. There is no difference between the preventive systems and countermeasures needed to recover from the global technological failures and those used when recovering from human-made catastrophes. Therefore, it is essential not to underestimate practical preventive mechanisms and the international dimension in cyber-security (Swaine, 2013).

At the regional and global levels, governments, global organizations, and ICT sector stakeholders need to do something such as forming formal cooperation networks as well as mechanisms for international incident response. The aim of this is to guarantee the capabilities of incident response when in case there is a global interruption.

2. New International Cyber Convention

Another disagreement concerns that are well-known make sure that new international cyber convection has been established. Countries such as Russia, Syria, and Iran, through their argument, supported a new legally binding international agreement. According to what was proposed by the Syrian representative, the agreement could include the establishment of an institutional mechanism or a permanent body that will be examining all relevant threats and issues in regards to using

[2] Tagert, A. C. (2010). *Cybersecurity challenges in developing nations* (Doctoral dissertation, figshare).

[3] Swaine, M. D. (2013). Chinese Views on Cybersecurity in Foreign Relations. *China Leadership Monitor*, *42*, 1-27.

ICTs in the international security context. Iran suggested that it would be essential if the agreement incorporates legal norms and rules with objectives that will ensure that there is no use of ICTs for malicious purposes (Geers, 2010).

The representative of Russia stated that the Kremlin does not want to change the existing international law. However, the representative feels that it is essential to adapt to that cyberspace law. While he analogized the international sea law, his argument stated that it is not impossible to declare that international law is applicable and, at the same time, come to an additional international agreement (Geers, 2010)[4].

However, a high number of representatives showed their desire to focus on understanding as well as the implementation of the rules that were agreed upon. The representative who represented Australia, however, raised a concern that certain cherry-picked areas will be the only ones that would be covered by that new convection, and overall, there will be lower protection of malicious cyber activities. Several nations, including the Netherlands and Canada, expressed their belief, stating that there is no need for new instruments and that the current norms are enough to guide the behavior of the State in the cyberspace. The representative of the United States recalled that international agreements are likely to take years and that these norms are likely to develop binding standards as time goes.

3. From Diverging Views to Common Interests

Apart from the above disagreements, the meeting also exposed potentially divergent views that are related to human rights, regulations of social media content, and offensive cyber capabilities developments.

Beyond the new convection need, representatives of states did not comment on issues that the whole international community does not share. The debate was focusing on identifying areas that future discussions would discuss at the OEWG (Achten, 2019).

There was a positive and engaging atmosphere during the debates, and this is according to tweets by the representative of States as well as the OEWG chair. It will be essential and necessary to ensure that constructive and sincere engagement is maintained among states in order to reach an agreement that is going beyond the mere reaffirmation that the international norms and law can be applied in the environment of ICT. The motto, "we are not starting from scratch," would be a perfect approach for the first meeting. In order to prevent positive ICTs' aspects, it will now be necessary for identifying concrete measures. Required by this is the assessment of the common interest and not putting the focus on national interests only. The OEWG

[4] Geers, K. (2010). Cyberweapons convention. *Computer law & security review*, *26*(5), 547 551.

representatives thus came to an agreement that it is necessary to understand better the existing norms precisely as well as identifying practices best for their implementation (Achten, 2019)[5].

4. Next Steps

February 2020 is when the next OEWG meeting will take place, and there is a possibility of including another round of open discussions. Before this year ends, there will be separate meetings that will be held by GGE. However, the complementary roles of both groups are yet to be established. The states that had the most contributions in the first session of the OEWG are also members of GGE. It is refreshing when we hear that some states are members of the smaller GGE. Their views could lead to the contribution of the mitigation of disagreements (Achten, 2019).

There is hope that there will be furthering of understanding and implementation of agreed norms by OEWG. However, the definition of the precise scope of further debates is yet to take place. The question is whether the OEWG is going to address how the nations behave in cyberspace, or it will include the examination of how non-state actors behave. The other question is whether it will address emerging technology-related issues. The other question is whether it will work together with regional bodies that are in the cyberspace sector. The fact is that disagreement will be there. However, a hope that a debate regarding norms related to international cyber could progress in the future was created by the OEWG meeting(Achten, 2019).

5. Pledge by 27 nations on cyber-security

Twenty-seven nations signed a statement[6], and they reaffirmed their commitment to constructing a framework where nations should be responsible in the cyberspace. This statement created a framework for nations, and the framework aims to show that the countries are continuing to support the international rules as well as encouraging its adherence, further development as well as the implementation, and included in this is an ongoing U.N. negotiation relating to the open-ended working group as well Government experts (Olenick, 2019).

This is what countries said in the statement that the U.S. State Department issued, "We support targeted cyber-security capacity building to ensure that all responsible

[5] Achten, N. (2019). New U.N. Debate on Cybersecurity in the Context of International Security. *Cyber and Technology*.Retrieved from https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-security.

[6] Olenick D. (2019). Twenty-seven nations ink cyber-security pledge. Retrieved from https://www.scmagazineuk.com/27-nations-ink-cyber-security-pledge/article/1660686.

states can implement this framework and better protect their networks from significant disruptive, destructive or otherwise destabilizing cyber activity. We reiterate that human rights apply and must be respected and protected by states online, as well as offline, including when addressing cyber-security" (Olenick, 2019).

Many countries signed this statement, and these countries are Canada, Italy, Denmark, Australia, Columbia, Estonia, Belgium, Czech Republic, Finland, France, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, The Netherlands, New Zealand, Norway, Poland, Korea Republic, Romania, Slovakia, Spain, Sweden, The United States and the United Kingdom (Olenick, 2019).

This statement is providing a support structure for the U.S. as well as our allies in order to further help in uniting and coordinating cyber efforts to defend our infrastructure from hackers that are aided by nations. Also, it will help in our citizens' protection against the ongoing operations of information by Russia as well as other adversaries (Words of Rosa Smothers, senior, V.P. of cyber operation at KnowB4. The group said that it is ready to work as a team to hold states responsible when they act against those principles by taking measures that they are consistent and transparent with the universal law. The pledge stated that there should be penalties in cyberspace for bad behaviors. This was announced when the United Nations General Assembly was to meet in New York (Olenick, 2019).

6. Norm, ICTs, and global security and peace

The classical definition of a norm is a mutual expectation for the right conduct of the individuals with a specific identity. It infers identity questions (assembling at which a norm is indicated), behaviors (that can be constructive, generative, and regulative), propriety (defines the behavior whether it is inappropriate and appropriate), and then mutual expectations (which are the norm's intersubjective and social character). Therefore, norms embody potent expectations that can compel and constrain individuals in global politics hence provides guidance on what is prohibited, needed, or permitted and consequently are deliberated to carry moral weight. Norms in international politics mirror the international community's expectations, set policies for accountable behavior of the State, and give permission to the worldwide community to investigate the states' intentions and the activities (Independent Commission on Multilateralism, 2016).

Some norms rely on the law for their propriety, others are formed to shape the law eventually, and others may evolve form religion, professional training, culture, and political consensus. If early efforts of articulating a norm as well as arrange supports around it succeed, it may touch a point of tip thus leading to the norm's cascade and its internationalization, that is put into action. The target follows the process of dynamic where a norm evolves and the behavior it is proscribing, and then grouping can be lengthy and complicated. The present worldwide context for mitigating the impacts of the above-mentioned international security and peace' cyber securities is extensive, with interests and responsibly spanning various global regimes and engaging various confidence-building and shaping of the norm processes also crucial investments in building capacity. Just like other places, growth is represented by positions that are oft-conflicting and interests of the non-state and State actors similar that inhibit collaboration and cooperation and persistent vulnerabilities in information communication technology (Independent Commission on Multilateralism, 2016).

Around the United Nations, very many sectors are involved in relevant information communication technology shaping of the norm, capacity, and confidence-building methods.

Regarding significant protection of the infrastructure, the second committee has worked as the first home for framing resolutions regarding the global culture's promotion of cybersecurity as well as significant infrastructure protection since the governmental expert group took up. Recently, for the first time, the Security Council was briefed though the "Arria formula" open meeting. Concerning the ICTs application and international security and peace that includes attacks associated with critical infrastructure. The third committee of the General Assembly, as well as the Economic and Social Council, have eyed on issues affecting human rights resulting from ICTs application. And not a per se of the cybersecurity, the subsidiary bodies of Security Council and itself have paid growing attention concerning questions affecting ICTS and internet usage for terrorism purposes within which a cooperative and a significant normative framework are evolving. The third and the second committees of the General assembly have eyed on normative base strengthening for responding to multinational assaults like using ICT and the Internet for criminal and terrorism. In the meantime, a good number of specialized agencies and departments are involved in some of those norms into practice, giving the member states support via raising awareness, building capacity, guidance, the rule of law, and technical assistance (Independent Commission on Multilateralism, 2016).

In the direction of the United Nations, the efforts to build confidence and shape norms amongst the states in response to insecurities related to ICT have become to be significant to other regional and international bodies. These comprise of efforts that aim at curtailing the risk of conflict arising from the ICTs. That is, outlining what the response must be in the incident of the ICT event, crucial infrastructure, or global financial services' strengthening, dealing with digital risk, enhancing cooperation to respond to the use of Internet and ICTs by the criminals and terrorists. They are comprised of African Union, Russian Federation, India, China, the European Union, the Organization of American States, the ASEAN Regional Forum (ARF), the Organization for Economic Co-operation and Development, the Council of Europe, South Africa grouping, the Group of 20, the Group of Seven, Shanghai Cooperation Organization, and Organization for Security and Co-operation in Europe, and Brazil.

The increasing number of actors provides building capacity support as well as technical assistance to aid the efforts of the states to implement these and other measures that are related at the national and regional stages.

These normative processes, as well as related cooperative efforts, capacity building, and confidence-building combine with the present governments, that is, law enforcement, international law fields, cable infrastructure, intellectual property, telecommunications, trade, and finance to create a various regime complex for dealing with international activities. This significantly means that the success of any process pf norm development will rely on how the states relate with other regimes as well as norm-shaping and process implementation evolving within. A conspicuous instance of this is how persevering differences amongst the states on primary principles and rules of the United Nations' role or international law in dealing with a crisis keep on spilling over into the ICT territory (Independent Commission on Multilateralism, 2016).

Whereas the regime complex may seem fragmented or cacophonous, significant has, however, been put in place on numerous fronts. For instance, on the front of the political-military until lately, the national expert groups (GGE)'s work had emerged from a highly conceptual conversation regarding controlling information weapons towards international law' confirmation and articulation and identification of specific State's behavior in the ICTs applications that has extended to other administrations. This has influenced the efforts of confidence-building at the levels or regions through the Organization of American States, Organization for Security and Co-operation in Europe, and ASEAN Regional Forum and has provided a critical background for the capacity building identification needs within various states. The same assumptions can be raised following the normative base evolving about human rights norms on ICT expressed lately and in response to the terrorist's and criminals' use of the ICTs and the Internet (Satola & Judy, 2010)[7].

These initial outlines can serve as crucial guidance for nations as they develop their national strategies that can contribute to better international security and stability. As shown by the GGE's failure in 2017 to attain a consent report, significant divisions amongst states continue, some of being technical or legal, and many of them being political. Some of the evolving norms indeed appear to be cascading or spreading only within particular subgroups, sometimes with setbacks around the same groups and continue to be contested somewhere else. The same remarks can be made regarding other normative procedures. Getting to a point where norms are internalized, cascaded, and spread at the national level, and ongoing disagreements are bridged, will remain the testing principle henceforth requiring crucial investments in building capacity and

[7] Satola, D., & Judy, H. L. (2010). Towards a dynamic approach to enhancing international cooperation and collaboration in cybersecurity legal frameworks: reflections on the proceedings of the workshop on cybersecurity legal issues at the 2010 United Nations Internet Governance Forum. *Wm. Mitchell L. Rev.*, *37*, 1745.

diplomatic action. The continued efforts in capacity building, as well as trust, involvement amongst the states, dialogue, and engagement between across regimes, between states, and other actors, are imperative.

7. The United Nations, ICTs, and International Security and Peace

Until recently there was an overall perception that no matter the ICTs complexity and growth in their malicious use that includes the states, progress which is good had been made in attaining consent on the norms, both non-binding and binding, applicable to the ICTs' use and coming up with a framework for ensuring a secure and stable environment for ICT. The majority of these deliberations have taken place within the First Committee of General Assembly regarding international security, GGEs, and disarmament, the subsequent framework then endorsed, picked up, or operationalized by various plurilateral, subregional, regional, and specialized bodies as well as a mutual agreement amongst the states (UNIDIR, 2017)[8].

8. The origin of the norm-shaping efforts of ICT in the framework of international peace and security

For decades, the General Assembly has been crucial for diplomatic discussions over information technologies and their professed and real effects, mainly as they connect to the sovereignty concept. Therefore, it was only natural that cyberspace and ICTSs that includes the Internet would arrive at its goal. Up to date, the majority of the United Nations discussions that relate to ICTs in the framework of international security and peace stimulated by a draft resolution tabled in the year 1998 by the Russian Federation. Closely following on the initial revolution's heels, in the year 2000, it anticipated International Information Security's principle that would form a foundation of a novel legal instrument to regulate how the states use ICT intending to protect surrounding information and illegalization of information weapons. The initiative evolved against Russian's background concerns over the alleged information technology sector' western dominance. Especially it is related to concerns over the military superiority of the United States coming from its information technology advancement in the military that became apparent in the year 1991 during a Gulf War and the increasing emphasis in the strategy of the western military on information dominance, information operations, and information warfare (Johnson, 2015)[9].

[8] UNIDIR. (2017). The United Nations, Cyberspace, and International Peace and Security.*Responding to Complexity in the 21st Century.*

[9] Johnson, T. A. (Ed.). (2015). *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare*. CRC Press.

The states' increasing number aided the efforts by the Russian Federations to shape worldwide legal regimes in intercontinental information security, and they were met with disbelief by the Western states (Newmeyer, 2015)[10]. This was in large reportedly because of the emphasis of the draft resolution on the information *per se,* the possible implication of human rights of that emphasis and the crucial role that the suggested regime afforded multilateral organizations and governments in managing ICT risk and insecurities without mentioning non-State actors' role like the technical organizations and private companies play in their organization as well as resolution. Some countries were reticent to deliberate the information security' information with a decommissioning framework. It risked initiating the worldwide community on a complex enterprise surrounding numerous interrelated factors that were not addressed by the first committee. Ordinarily, that is technical aspects that relate to international communications and nontechnical problems linked with antiterrorist cooperation, economic trade and cooperation, law enforcement, intellectual property rights, and other issues that were regarded in the sixth or second committee. Other states stated that information focus instead of cybersecurity placed content instead of infrastructure at the debate's center. The determination would have placed conversation on ICT capabilities as well as invited the public inspection of the ICT abilities, a stage at which no state with the technologically sophisticated military was ready to take. Numerous efforts to slice the matter, pushing it out of the first committee then to the second and then to the third one failed. As one way to push this conversation forward, the Federation of Russia proposed the formation of the GGE to discuss the matter (UNIDIR, 2017).

9. State of the art in Italy

Cyber-security is the undisputed arbiter of the game globally but also locally as Italy. The constant growth and increasing of interconnected devices and sensors, threat points and vectors are multiplying, and the exposed attack surfaces of critical infrastructures are particularly vulnerable, during the COVID 19 pandemic several attacks where carried out in particular against hospitals.

Think about what could happen due to a cybernetic compromise of essential services such as Hospitals, or rails; or again, to the consequences of the intrusion and control of the safety systems of power plants, or following a significant blackout, the tampering of the restart sequence of the energy chain. Staying "abreast" of the State of the art in terms of cyber-security is therefore not an option, but a necessity – here too, the current data for the country is not exactly encouraging, showing an overall capacity

[10] Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal*, *1*(3), 9-19.

of mediocre scope: according to a recent Comparitech11 study on 60 countries, Italy would rank 36th between Argentina (better than us) and Malaysia.

The topic of cybersecurity is one of the topics that governments and businesses are increasingly considering a priority for the well-being of a nation and the protection of citizens, freedom, and businesses.

This low level of cybersecurity preparation of the country system is inexorably reflected in a low awareness among citizens-users; we all use daily smart devices that allow us to have everything at our fingertips but what we neglect is that at the same time we are also within everyone's reach, and not everyone has benevolent intentions, just think of the numerous malware that was widespread during this pandemic. In the face of an enormously amplified exposure to the world, through multichannel and interconnection of global networks, mirroring accessibility corresponds to a tremendous amount of content, which before we could not even imagine; but "great power derives great responsibilities," in particular information and content appropriately, defending ourselves from misinformation and fake-news that manipulate our knowledge.

Italy adopted the DL CYBER – as an instrument to prevent this threat and provide an answer.

The Italian Government, with the Law Decree n. 105 of 2019 has strengthened its cybersecurity strategy. The Government received the NIS Directive by imposing security duties to entities that would fall out of the scope of application of the NIS Directive. The NIS Directive shows the operators of essential services (i.e., energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructure), including them in a specific list.

The "Cybersecurity Perimeter," includes all private and public operators and service providers with a legal entity in Italy, which are considered essential for the well-functioning and the interest of the State, whose disfunction, interruption or illegal use would compromise national security with social and economic impacts.

The PerimeterPerimeter introduces a cybersecurity framework, which shall be detailed by way of specific measures that will be set out in the same Prime Minister's decree and that the entities comprised in the PerimeterPerimeter will be obliged to adopt, in order to attain an adequate level of cybersecurity specifically with reference on security management, the mitigation of incidents and their prevention, the physical and logic protection of data, the network integrity, training and awareness of staff.

An important role is played by the CVCN (which stands for Centro di Valutazione e Certificazione Nazionale), which is a supervisory body under the control of the Ministry of Economic Development or entitled bodies that respects the legal and technical requirements.

[11] https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.

This critical introduction act directly on Public Procurement to purchase ICT equipment that needs to do a risk analysis based on its intended use, which means integrity checking. The CVCN may authorize the purchase or impose preliminary verifications, binding conditions, and tests considering the risks involved following the certification's schemes following ENISA and international standards that indicate the following areas:

organizational structure dedicated to security management;

- security and risk management policies;
- mitigation, management, and prevention of incidents, including through interventions on devices or products that are seriously inadequate from a security standpoint;
- logical and physical data protection;
- integrity of I.T. networks and systems;
- operational management, with specific regard to continuity of service;
- monitoring, testing, and control;
- training and awareness;
- assignment of contracts for the supply of information and communication technology (ICT) goods, systems, and services, including through the definition of general characteristics and requisites.

In case of non-compliance, entities included in the Perimeter will be exposed to severe administrative monetary sanctions from 200,000 up to 1,800,000 Euros in case of infringement of the duties imposed by law and the CVCN's and of the Government's prescriptions. False communications to CVC during the purchase of ICT equipment or Government's inspection is considered a crime, which might be punished with imprisonment for up to 3 years according to the law.

The PerimeterPerimeter reinforced the "Golden Power," an instrument to allow the “veto” power on any possible acquisition of providers operating in Italy from international bodies.

Concluding, Italy identified the strategy, now it is time to act and transform these rules in actions, Italy due to the geopolitical role played cannot miss this opportunity to start a new way to provide strategic services adopting necessary cybersecurity measures in order to guarantee their citizens, institutions and also the foreign direct investments that consider these requirements fundamental.