Stella Blumfelde

The role of international organizations in global cybersecurity governance

THE ROLE OF INTERNATIONAL ORGANIZATIONS IN GLOBAL CYBERSECURITY GOVERNANCE

How do international organizations govern cybersecurity? While there is an extensive literature on international organizations and security governance, there is little written about how they manage and adapt existing governance mechanisms to new threats. International security environment has been radically reshaped particularly by the growing number of Internet users, increasing interconnectedness and cybercrime activity. In this light, cybersecurity governance has emerged as a combination of overlapping issues of technical, political, and legal nature, creating a conflict of differing discourses, values, and governance models. While cybersecurity governance literature can be largely divided focusing on either the role of the state or non-state actors, Un has been increasingly highlighting the importance of international organizations, in particular regional organizations, as the contributors of security. This paper addresses the gap in international organization and cyber studies literature by a comparative analysis of global cybersecurity strategies. This paper provides an insight into already existing security governance frameworks relying upon specific mechanisms as mediation, peace operations, disarmament, and collective security for both traditional and contemporary issues. To observe possible differences or similarities in global cybersecurity governance, the paper analyzes further in more detail the security governance mechanisms applied by international organizations in governing technology such as nuclear, conventional, and lethal autonomous weapons. Finally, the paper concludes by highlighting resilience framework, typically applied in security governance of technologies, commonly used by international organizations also to govern such threats of unpredictable nature as those of cyberspace.

KEYWORDS *International Organizations, International Relations, Security Governance, Cybersecurity, Resilience.*

1. Introduction

The concept of security is one of the most contested topics not only in academia but also in international politics. Its complex nature and tendency to be overlooked from the state-centered military perspective has hampered

Stella Blumfelde, University of Genoa, Department of Political and International Science – Albergo dei Poveri, Piazzale E. Brignole, 3a – 16126 Genoa, email: stella.blumfelde@edu.unige.it, orcid: 0000-0003-3521-5194.

ISSN 2785-0072
© Società editrice il Mulino

its appropriate understanding (Buzan 1983). While nowadays security governance has expanded to comprise environmental, economic, societal, and political issues managed by a variety of actors (Buzan *et al.* 1998, 7-8), it is the advancement of Information and communication technologies (Icts) and cyberspace that has modified the nature of security governance. Despite the general recognition of the importance of international cooperation in cyber threat management, a global approach to cybersecurity remains a challenge for the international community due to the rapidly changing nature of cyberspace as well as its ambiguous terrestrial and non-physical characteristics requiring technical knowledge.

The changing nature of threats in International relations (Ir) has surpassed the capacity of individual states to provide security, therefore fostering the emergence of a security governance system of «governance without government» (Rosenau and Czempiel 1992). At the heart of this system, international organizations (Ios) have experienced a more prominent role as security governance providers by extending the scope of their traditionally limited mandates (Kirchner and Dominguez 2011). While some scholars dismiss the importance of Ios within this system (Mearsheimer 1994; Waltz 1979), others confirm their pacifying role in international politics establishing an interconnected governance network through a set of rules, norms, and procedures (Dorussen and Ward 2008; Hinsley 1963; Keohane 1993; Ruggie 1992). The manifold financial, monetary, expertise, and technical resources an Io can possess grants them the capacity to set global governance agenda, as well as shape and influence how governments and society articulate commonly shared concerns on global matters (Finnemore and Sikkink 1998; Keohane 1989; Majone 1997).

In the light of the changing nature of security threats and their governance, the key aim of this article is to explore the role of Ios in global cybersecurity governance. The findings of the paper on one hand identify resilience framework as an increasingly applied security governance mechanism for ambiguous contemporary security threats such as cybersecurity. On the other hand, they demonstrate that as unique as cyberspace is, it shares similar challenges faced in the governance of other technologies and therefore does not present itself as a completely foreign area of management. For the scope of this paper, I first examine previous and current Ir literature addressing the role of Ios in security governance. By focusing on existing treaties and Io strategies for technologies such as nuclear, conventional, and lethal autonomous weapons, I then compare Io security governance approaches to cybersecurity by examining relevant official documents and strategies of the Un and its bodies. With this evaluation I highlight resilience framework as commonly applied security

governance mechanism by Ios. What this article does not do is evaluate the cybersecurity governance structure in its entirety due to the multiplicity of actors involved in cybersecurity provision. Instead, only the key international bodies and regulations have been included in the analysis.

2. International organizations and security provision

Historically, Ios were seen as tools for intergovernmental cooperation in resolving primarily issues of security and peace (Archer 2001; Karns *et al.* 2015). The current framework for international security governance was established within two international diplomatic conferences held in the 19th century. The Vienna congress paved the way for the institutionalization of periodic meetings as means for deterrence of aggression (Nicolson 1942, 32-33). The Hague conferences, on the other hand, established the foundations for contemporary security governance mechanisms within one of its Conventions on pacific settlement of disputes (1907). Amongst the primary dispute settlement mechanisms, also known as preventive diplomacy aiming to prevent development, escalation or spreading of a conflict, mentioned in the Convention are mediation, investigation, and arbitration by a third-party actor. These mechanisms were incorporated within the activity of the United nations (Un) (Boutros-Ghali 1992, 45; Un 1945a), as well as various regional intergovernmental organizations (Igos), and non-governmental organizations (Ngos). The League of nations, which had the key role in conflict resolution in the 20th century, extended the traditional security governance tools of mediation, arbitration, and investigation, to the establishment of sanctions in case of a dispute, collective security, and disarmament. These mechanisms were later adopted by the Un (Un 1945b).

International sanctions are one of the key enforcement instruments applied by Ios that aim to change a behavior of an actor or punish it by constraining its access to critical goods and funds, to signal the importance of international norms (Biersteker 2013; Schmitt 2016). Most commonly, the norms that are signaled through sanctioning are the prohibition of war and armed conflict, human rights, counterterrorism, non-constitutional changes in government, and nuclear nonproliferation (Biersteker 2013). Collective security, similarly, aims to manage state behavior through peaceful negotiation, collective confrontation of the aggressors, and mutual trust, instead of the use of military force (Claude 1963). However, while collective security is the core design function of most Ios, including the Un (Un 1945c), Io security provision capacity based upon this mechanism is skeptically viewed within Ir (Barkin

2013). Whereas collective security proposes to confront aggressors with too much to fight against, disarmament proposes to deprive nations of anything to fight with. It eliminates the means by which it is possible to wage war with the aim of establishing trust between actors through common norms and information exchange.

In the light of the difficulty to control or predict future threats, security management has been increasingly discussed within the context of resilience and the adaptive and recovery practices developed for possible or unforeseen security risk threats (Petersen 2016). Resilience framework is widely applied to a broad range of threats emanating from security crises such as conflict, poverty, or environmental issues. Instead of dealing with security issues when manifested, the concept of resilience seeks to address the capacities of security targets themselves to provide to these communities the needed skills and solutions to understand, to cope with and to eventually manage security threats. In particular, the concept of resilience can be found in such security governance mechanisms applied by Ios as peacekeeping and peacebuilding (Fortna 2004; Paris 2004). Peacekeeping has the potential to create a stable environment of conflict in which peace agreements can be achieved, local populations at risk can be protected, as well as foundations established for a long-term peace. The practice of state-building or peacebuilding not only involves the oversight of post-conflict areas but also provides capacity building of the locals and their governance systems. What distinguishes it from other mechanisms is that it has a preventive rather than enforced nature as through capacity-building threats to international security are expected not to degenerate into a security-threatening environment.

The presence of global security governance mechanisms places forward the issue of security dilemma, which refers to an environment of constant insecurity caused by misperception of the development of security capabilities that while being defensive in nature, might seem potentially offensive to another state causing it to develop counter-response (Buzan and Hansen 2009). This is where Ios play a significant role in minimizing the issue of misperception and potential inter-state conflict through deterrence of aggression by mediation, arbitration, monitoring of compliance, and the promotion of common norms (Barnett and Finnemore 1998; Duvall and Wendt 1989; Keohane 1984; Mearsheimer 1994). Many Ios, in fact, can be observed to apply several of these mechanisms simultaneously. However, world politics today are distant from the traditional perspectives of security as global governance cannot be seen solely through the lens of state actors and the great power politics, despite their prevalence. Moreover, various issues have developed to adopt a transborderless nature that cannot be any more limited to national territories.

3. International organizations and security governance of technologies

Security governance has expanded to include various complementary organizations and agencies with often differing areas of work, like in the case of cybersecurity. The next paragraphs, comparing Io strategies for conventional, nuclear, and lethal autonomous weapons systems, find that the prevalent security mechanism in global governance of these technologies is capacity and confidence building. This mechanism includes such tools as training provision on legal and regulatory issues, human resource knowledge development, adherence to common norms and regulations, arms controls and finally, information exchange on materials, facilities, and national capabilities potentially harmful for international peace and security. This comparative analysis will give me the opportunity to observe how and if global cybersecurity governance differs from already existing similar governance regimes of technologies.

Nuclear weapons

Similarly to Icts, the dual-use nature of nuclear technologies requires the division of their governance into two distinct branches - the first one being the technical or nuclear safety addressing physical protection of nuclear materials and equipment, and the second being political strategy or non-proliferation and disarmament referring to the prevention of nuclear weapons and their components spreading to state or non-state actors. However, unlike cybersecurity governance, nuclear is governed not only by voluntary codes of conduct, but also by legally binding treaties.

While security governance of atomic energy was first outlined by the Un (Unga 1946), the primary Io that manages nuclear materials is the International atomic energy agency (Iaea). Its designated nuclear non-proliferation treaty (Npt) (Iaea 1970) is at the center of the global nuclear nonproliferation governance system. Registration and inspection of nuclear stockpiles together with verification of adherence to international law are the key governance mechanisms, also known as confidence building measures (Cmbs), set out in the Treaty is the Safeguards system and supported by the Un through the adoption of sanctions (Unsc 2015). Additionally to Cbms, Iaea promotes capacity-building mechanisms such as training on legal and regulatory issues; software, equipment, and human resource knowledge development, and awareness building.

Besides the Iaea and Un, also regional Ios contribute to nuclear governance. Generally, all of them follow the already established principles of

non-proliferation and disarmament such as Cbms and the normative guidelines and sanction regimes as set by the Un. Some of them apply additional governance mechanisms such as prohibition of any activity related to nuclear weapons through legally binding treaties (Asean 1997a; permanent council of the Oas 2016; Opanal 1967; Oau 2009; Treaty on a nuclear-weapon-free zone in central asia (Canwfz) (2009), export controls (European commission 2005; Nato 2022), and crisis response systems (Nato 2022).

Conventional arms

Unlike for nuclear weapons establishing strategies of disarmament, the main goal of conventional arms governance is the prevention of their misuse through the control of arms movement. While the Un sets common international standards for regulating international trade through Cbms such as national control systems and points of contact for information exchange, and capacity-building measures through assistance for institutional, legislative, and financial issues (Un 2014; Unga 2019b; Unroca n.d.), it differentiates between measures taken at national, regional, or global level. At the global level, the Un promotes the implementation of arms embargoes (Unga 2001), information exchange, capacity-building in identification of illicit arms (Un 2005; Unga 2001), the development of appropriate legislation, and training of human resources. At the regional level, the Un encourages the establishment of points of contact and enforcement bodies for the purposes of information and expertise sharing (Un 2001).

As with global nuclear security governance, regional Io efforts are highlighted as crucial in combating the proliferation of arms as many had already an established framework addressing arms control before the agenda offered by the Un (Asean 1997b; Au 2000; Nato 1995; Oas 1997; council of the Eu 2008). The most noteworthy regional nuclear governance mechanisms are the Treaty on conventional forces in europe (Cfe) regulating military equipment (Osce 1990), the Vienna document outlining Cbms for military activities (Osce 2011) and the Open skies treaty supporting the previous Cbms with unarmed aerial observation flights (Osce 1992).

While generally all regional organizations follow the Un and Osce security governance framework based upon information and best practice sharing, legislative and technical assistance, only the Eu, Osce, Au, League of Arab states and Ecowas have implemented arms embargoes (Sipri n.d.).

Lethal Autonomous Weapon Systems

The most recent development in the global security governance of technologies is the Lethal autonomous weapon systems (Laws). Laws pose significant risks in the context of the accountability gap in the targeting cycle, which is the system inability to distinguish between combatants and civilians on the battlefield (Nato Rto 2007; Unidir 2014). This issue affects the ability to comply with the principle of discrimination of the International humanitarian law (Ihl) (Icrc 2016, p. 16). Moreover, Laws might create the risk of unintended escalation as the actions of automated systems might be unforeseen or unpredictable. Finally, the competitive technological development dynamic could accelerate Laws development and deployment before any testing could be done (Horowitz 2019).

Since 2016, the Un has an established Group of governmental experts (Gge) on Laws (high contracting parties to the Ccw 2016), seeking to adapt the framework of Ccw to emerging technologies. Currently, the only governing mechanism of Laws is a set of 11 guiding principles and norms endorsing international and Ihl, and human responsibility over weapon systems based on emerging technology (Un 2019). The Un Gge on Laws continues its work in clarifying how exactly international law may be applied to the governance of emerging technologies, as well as whether legally binding instruments should be applied for the global governance of Laws (Un Gge 2022).

4. International organizations and cybersecurity governance

The consistently evolving global security environment consisting of new concepts, measures, security perspectives and understandings, as well as actors that stretch beyond the state as the traditional player in Ir, has created an ongoing multi-layered debate on questions of legal, ethical, conceptual, political, and overall, also organizational issues on cyberspace security governance. In the light of the growing role of Ios in global security governance, the following part of this paper explores the role of Ios, in particular, the Un and its bodies, in the governance of cybersecurity.

In the Sixties, the Internet emerged as a Us government funded project with the aim to establish a resilient and secure network for quick communication in national defense which would later become the foundation of the Internet (Waldrop 2015). In 1986, the development of the Internet was handed to the Internet engineering task force that operated without governmental

supervision and adopted a cooperative decision-making process involving not only governmental, but also non-governmental representatives in the identification of engineering issues (Fidler and Mundy 2020, pp. 66-67). In 1998, as a response to the incapability of private sector to provide support and coordination for various cyberspace vulnerabilities and technical services critical to the operation of the Internet, a multistakeholder cybersecurity governance regime emerged with the establishment of the Internet corporation for assigned names and numbers (Icann) (Icann 2013, p. 2). The same year, the Un recognized Icts as a threat to international security and stability (Russian Federation 1998), therefore extending the initial technical focus of the Internet governance on the management of the Internet identifiers and the exclusive role of Icann over these processes. The World summit on the information society declared the development of shared principles, norms, rules, decision-making procedures, and programmes for the Internet as of the primary responsibility of governments. Ios, on the other hand, was acknowledged to have a complementary role in the development of Internet-related technical standards and policies (Itu 2005; Mueller 2017). Nowadays the Un declares itself as the leading actor in ensuring intergovernmental cooperation through the development of common understanding on the security and use of Icts, as well as the application of international law, norms, rules, and principles for responsible State behaviour in cyberspace (Unga 2015).

These historical dynamics have resulted in a clash of perspectives on what to secure in cyberspace between different communities of actors creating a distinction between Internet and cybersecurity governance (DeNardis 2014; Mueller 2017). Nowadays, Internet governance has become an umbrella term to a wide array of technical, political and legal security issues, becoming difficult to distinguish it from the processes of cybersecurity, which has created a conflict of differing discourses, values, as well as governance models (Calderaro 2021; Cavelty Dunn 2008; Mueller 2017). However, while Internet governance remains the responsibility of Icann, and therefore deals with the functioning of the Internet and its networks, the Un leads the global cybersecurity governance through the Group of governmental experts examining the issue of information security from a national security perspective (Russian Federation 1998).

The potential misuse of Icts for criminal and terrorist purposes, and national development of Ict capabilities for military purposes are seen as the most significant threats in cyberspace (Unga 2006; Unga 2015). In the light of these cyber threats, Un Gge has outlined the global cybersecurity governance by developing 11 voluntary and non-binding norms in the context of responsible behaviour of States in the use of Icts that base upon the applicability of interna-

tional law (Unga 2014 2015). The norms established by Un Gge have been further endorsed by other international regional agencies such as Osce and Asean.

Besides norms, Un Gge supports the applicability of Cbms in cyberspace as set in the Guidelines adopted by the Disarmament commission (1988). Cbms for cyberspace can be largely divided into three groups of action: the identification of national policy and technical points of contact; information and best practice exchange; and finally, national view exchange on political, legislative, and normative measures implied to protect critical infrastructure (Unga 2015, p. 9).

Additionally to Cbms, Un gge emphasizes the importance of capacity building and technical assistance in Ict and international security (Unga 2011; Unga 2019a). Such measures can include cooperation between relevant agencies to address Ict security incidents through the development of technical, legal, and diplomatic mechanisms of information and human resource exchange, as well as provision of assistance in investigation of Ict incidents by establishing national computer emergency response teams (Unga 2015).

Lastly besides issues of state behavior in cyberspace and cybercrime, since the release of the Un secretary-general's Agenda for disarmament (Unoda 2018), also disarmament, although limited to the need to contribute to the prevention and peaceful settlement of conflict within cyberspace, has become an issue connected to cybersecurity governance.

The prevention of cyber threats has always been executed in cooperation between governments, the private sector and civil society facilitated by international and regional organizations (Unga 2002). While the idea of cooperation can be observed in all the Un general assembly resolutions on Icts and cybersecurity released since 1998, the documents make a particular reference to the complementary role of regional Igos in assisting the Un in developing a secure Ict environment through such governance mechanisms as capacity building, confidence-building, and exchange of best practices (Un Gge 2013; Unga 2015; Unga 2019a; Unsc 2006). In fact, while the Un has actively addressed the issue of cybercrime, the Council of Europe's Convention on cybercrime is the only legal instrument seeking to harmonize legal issues in cyberspace such as fraud, illegal interception, and others.

As the dynamics of Internet governance suggests, security, initially, was not organized through a formal institutional framework. For a long time, the threat and risk management were the responsibility of the private sector representing the governance of technical functioning of cyberspace. A multistakeholder cybersecurity governance regime emerged as a response to the private actor incapability to set coordinated information sharing networks and provide legal support to the breaches of cybersecurity. The different outlook on

cyber issues emanating from different communities of actors and their objects of security created a distinction between Internet governance and cybersecurity governance (DeNardis 2014; Mueller 2017). Internet governance emerged as a globally inclusive effort to narrow the digital divide between countries and to assist in advancing digital infrastructure through shared principles and programmes that shape the evolution and use of the Internet (Itu 2005, p. 4). At the same time, cybersecurity governance, based upon policies and risk management approaches securing Icts and their connected network environment (Itu 2009, p. 2), has run parallel to these processes as it was seen as an exclusively matter of individual states and experts due to its originally technical notion of threats and security (Mueller 2017). While different cyberspace security governance perspectives and strategies exist, nowadays they are all dominated by various global and regional Ios.

Resilience and cybersecurity governance

The broad applicability of the concept of resilience across various fields of issue, has resulted in the term embodying multiple meanings and indicators. While the term was originally applied in reference to ecological systems and disaster management in the context of the capacity to absorb change and the ability to return to an equilibrium state (Holling 1973), generally resilience refers to the ability of society or a system to cope with unanticipated external stresses and changes (Adger 2000; Allenby and Fink 2005; Rose and Liao 2005).

The applicability of the concept of resilience has become an increasingly prevalent issue also within cyber studies. In the realm of Ir, cyber resilience is of particular importance due to the interconnectedness of technology and the potentially far-reaching consequences of cyber attacks. Cyber resilience is the ability of a society or an organization to withstand and recover from cyber attacks or other disruptions to its technology and internet infrastructure (Itu-t 2015).

Despite the multidisciplinary nature of resilience, there are four common security framework features across all fields known as Tose – the technical dimension in reference to physical systems, organizational in reference to the capacity of organizations, social in reference to communities and governments, and finally, economic in reference to economic losses (Bruneau *et al.* 2003). Although the applicability of these dimensions in International security studies (Iss) is limited, the governmental capacity and ability to communicate to other authorities in case of an attack, to address cybercrime through legislation, to provide communication between the public and private sector, and to hold crisis management exercises and negotiations are seen as the main pillars of national cyber resilience (Falco *et al.* 2019; Tiirmaa-Klaar 2016). Moreover, while

scholars still debate on the possibility of cyber war, international cooperation and dialogue are seen as key security mechanisms in improving cyber resilience and reducing the risks of cyber attacks (Clarke and Knake 2011; Rid 2012).

While cyber crisis management and cyber resilience are prominent measures in national cybersecurity strategies, resilience frameworks are absent in the literature on international cybersecurity governance. The analysis of Io role in cybersecurity provision in this paper reveals that the historically technical nature of cyberspace has left its management dominated by practical tools such as capacity and confidence building (Unga 2015; 2019). The prevalence of these mechanisms in governing cyberspace are in line with the comparative analysis of security mechanism tools applied in governance of other technologies. However, due to the ambiguous nature of cyberspace, its security governance differs from that of other technologies with the widespread use of negotiations as a Cbms mechanism on common norms and principles of behavior in cyberspace as well as the applicability of international law in this domain (Unga 2015).

The concept of cyber resilience highlights the need for societies and organizations to be prepared for the potential impacts of cyber attacks. As the use of technology and the internet continues to grow, it is important to develop robust strategies addressing the prevention of threats. Cyber resilience, being a nascent but prominent discourse both within the academic and policymaking environment, still lacks an exact definition of its meaning in global cyber governance. Moreover, cyber resilience literature is dominated by technical security frameworks and therefore overshadowing social science tools to study cyber resilience and on how resilience in general applies to Ir. By examining the policies and strategies of Ios, we can gain a better understanding of the challenges and opportunities presented by the issue of cyber resilience in the global governance community.

5. Conclusion

As has the landscape of security actors changed over the years, so has the landscape of the threats. This has left Iss debating whether national domestic threats should be shifted or accompanied by the concept of international security, whether the study of referent objects of security should include others than the state, and whether the traditional focus on the use of force should extend to include other types of security fields and capabilities such as energy, science and technology, natural resources, and computer security. While the expansion of the concept of security can be seen as an interference with

the coherence of future research (Brown 1989; Buzan 1983), new technologies have taken a particular place within this debate as a driver of reassessment of threats, vulnerabilities, and strategies over the years in the discipline (Walt 1991). Moreover, the changing nature of security threats and their governance has surpassed the capacity of individual states as the sole providers of security. Ir literature emphasizes the role of Ios in global security governance due to their manifold financial, monetary, expertise, and technical resources allowing them to set the global agenda by shaping perceptions of governments and civil society (Finnemore and Sikkink 1998; Haftel and Thompson 2006; Keohane 1989; Majone 1997). In this light, the key aim of this paper was to explore the role of Ios in the governance of such ambiguous and nascent global security environments as cyberspace.

Historically, the main security governance tool of Ios as means for conflict resolution and deterrence of aggression have been governmental meetings. Over time their role became increasingly more active in signaling the importance of adherence to international norms through such preventive diplomacy and collective security mechanisms as mediation, investigation, and arbitration and introduced sanctions alongside such concepts as disarmament. The difficulty to control or predict future threats has extended the debate of security management beyond traditional notions of security to include concepts such as resilience addressing the capacity building of security targets. Resilience framework for security governance, initially practiced in peacekeeping and peacebuilding activities, nowadays is a prominent mechanism applied in the governance of various technologies such as nuclear and conventional weapons, as well as laws.

By comparing the security governance of various technologies, this paper reveals that cyberspace, while being a unique security environment to govern and to frame in the context of Ir due to the anonymity of the actors and their motivation in conducting crime, shares similar challenges faced in the governance of other technologies and therefore does not present itself as a completely foreign area of management. Characterized by rapid technological development and therefore, uncontrollable expansion of cyberspace, resilience framework prevails also in the governance of cybersecurity. As other security governance regimes for technologies analyzed in this paper, global cybersecurity is dominated by such capacity building mechanisms as training provision on legal and regulatory issues, and human resource knowledge development, often coupled with Cbms requiring the adherence to common norms and regulations, arms controls and information exchange on materials, facilities, and national capabilities potentially harmful for international peace and security.

Cybersecurity governance, as has been discussed in this paper, has developed overtime into an issue of differing discourses, values, as well as governance models shared between numerous different actors across the world, and it is affected by the constant evolution of technology which requires regular readoption of security measures. Ios are at the center of this continuously developing cybersecurity governance environment, choosing a resilience framework based on Cbms and capacity building as the key strategy for achieving international peace and security in cyberspace. Taking in mind the state-centric cyber studies and the lack of resilience debate in Ir, this paper aimed to provide an incentive for future research on emerging transborderless security governance issues by highlighting the relevant global role and security strategies of Ios. Further debate on Io cybersecurity governance and the applicability of Ir concepts to emerging issues could benefit from exploring the assigned complementary role and strategies of regional Ios by the Un in security provision (Unidir 2019; Un 1945; Unsc 2006).

References

Adger, W.N. (2000), *Social and Ecological Resilience: Are They Related?*, in «Progress in Human Geography», 24(3), pp. 347-364.

Allenby, B. and Fink, J. (2005), *Toward Inherently Secure and Resilient Societies*, in «Science», 309(5737), pp. 1034-1036.

Archer, C. (2001), *International Organisations*, London, Routledge.

Asean (1997a), *Treaty on the Southeast Asia Nuclear Weapon-Free Zone*, Bangkok, Asean, https://treaties.unoda.org/t/bangkok (last accessed on 11th December 2022).

Asean (1997b), *ASEAN Declaration on Transnational Crime*, Manila, Asean, https://asean.org/wp-content/uploads/2012/05/ASEAN-Declaration-on-Transnational-Crime-1997.pdf (last accessed on 11th December 2022).

Au (2000), *Bamako Declaration on an African Common Position on the Illicit Proliferation, Circulation and Trafficking of Small Arms and Light Weapons*, Bamako, Au, https://au.int/sites/default/files/documents/39250-doc-200._small_arms_and_light_weapons_in_africa._illicit_proliferation_circulation_and_trakkicking.pdf (last accessed on 11th December 2022).

Barkin, J.S. (2013), *International Organization: Theories and Institutions*, New York, Palgrave Macmillan.

Barnett, M. and Finnemore, M. (1998), *The Politics, Power, and Pathologies of International Organizations*, in «International Organization», 53(4), pp. 699-732.

Biersteker, T.J. (2013), *State, Sovereignty, and Territory*, in W. Carlsnaes, T. Risse and B.A. Simmons (eds.), *Handbook of International Relations*, London, Sage Publications, pp. 245-273.

Boutros-Ghali, B. (1992), *An Agenda for Peace: Preventive Diplomacy, Peacemaking, and Peace-Keeping*, New York, Un, https://digitallibrary.un.org/record/145749 (last accessed on 11th December 2022).

Brown, N. (1989), *Climate, Ecology and International Security*, in «Survival», 31(6), pp. 519-532.

Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O'rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A. and Von Winterfeldt, D. (2003), *A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities*, in «Earthquake Spectra», 19(4), pp. 733-752.

Buzan, B. (1983), *People, states, and fear: The National Security Problem in International Relations*, London, Wheatsheaf Books.

Buzan, B., Waever, O. and De Wilde, J. (1998), *Security: A New Framework for Analysis*, London, Lynne Rienner Publishers.

Buzan, B. and Hansen, L. (2009), *Defining International Security Studies*, in B. Buzan and L. Hansen, *The Evolution of International Security Studies*, Cambridge, Cambridge University Press, pp. 8-20.

Calderaro, A. (2021), *Diplomacy and Responsibilities in the Transnational Governance of the Cyber Domain*, in H. Hansen-Magnusson and A. Vetterlein (eds), *The Routledge Handbook on Responsibility in International Relations*, London, Routledge, pp. 394-405.

Cavelty Dunn, M. (2008), *Cybersecurity and Threat Politics: Us Efforts to Secure the Information Age*, London, Routledge.

Clarke, R.A. and Knake, R.K. (2011), *Cyber War: The Next Threat to National Security and What to Do About It*, New York, Harper Collins Publishers.

Claude, I.L. (1963), *Swords into Plowshares: The Problems and Progress of International Organization*, New York, Random House.

Council Of The Eu (2008), *Council Common Position on Defining Common Rules Governing Control of Exports of Military Technology and Equipment*, Eu, at: http://data.europa.eu/eli/compos/2008/944/oj/eng (last accessed on 12th December 2022).

First Hague Conference Convention for the Pacific Settlement of International Disputes (1907), https://avalon.law.yale.edu/20th_century/pacific.asp (accessed on 11th December 2022).

Denardis, L. (2014), *Global War for Internet Governance*, New Haven, Yale University Press.

Dorussen, H. and Ward, H. (2008), *Intergovernmental Organizations and the Kantian Peace: A Network Perspective*, in «Journal of Conflict Resolution», 52(2), pp. 189-212.

Duvall, R.D. and Wendt, A. (1989), *Institutions and International Order: Approaches to World Politics for the 1990s*, in E. Czempiel and J.N. Rosenau (eds.), *Global Changes and Theoretical Challenges*, Lanham, Lexington Books, pp. 51-73.

European Commission (2005), *Regulation on the application of Euratom safeguards*, Eu, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32005R0302 (last accessed on 12th December 2022).

Falco, G., Noriega, A. and Susskind, L. (2019), *Cyber Negotiation: A Cyber Risk Management Approach to Defend Urban Critical Infrastructure from Cyberattacks*, in «Journal of Cyber Policy», 4(1), pp. 90-116.

Fidler, B. and Mundy, R. (2020), *The Creation and Administration of Unique Identifiers*, 1967-2017, Icann, https://www.icann.org/en/system/files/files/creation-administration-unique-identifiers-1967-2017-18nov20-en.pdf (last accessed on 12th December 2022).

Finnemore, M. and Sikkink, K. (1998), *International Norm Dynamics and Political Change,* in «International Organization», 52(4), pp. 887-917.

Fortna, V.P. (2004), *Does Peacekeeping Keep Peace? International Intervention and the Duration of Peace After Civil War*, in «International Studies Quarterly», 48(2), pp. 269-292.

Haftel, Y.Z. and Thompson, A. (2006), *The Independence of International Organizations: Concept and Applications*, in «The Journal of Conflict Resolution», 50(2), pp. 253-275.

High Contracting Parties To The Ccw (2016), *Report of the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (Laws)*, Geneva, Un, at: https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=CCW/CONF.V/2&Lang=E (last accessed on 12th December 2022).

Hinsley, F.H. (1963), *Power and the Pursuit of Peace: Theory and Practice in the History of Relations between States*, Cambridge, Cambridge University Press.

Holling, C.S. (1973), *Resilience and Stability of Ecological Systems*, in «Annual Review of Ecology and Systematics», 4, pp. 1-23.

Horowitz, M.C. (2019), *When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability*, in «Journal of Strategic Studies», 42(6), pp. 764-788.

Iaea (1970), *Treaty on the Non-Proliferation of Nuclear Weapons*, Iaea, https://www.iaea.org/sites/default/files/publications/documents/infcircs/1970/infcirc140.pdf (last accessed on 12th December 2022).

Icann (2013), *Beginner's Guide to Participating in Icann*, Icann, https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf (last accessed on 12th December 2022).

Icrc (2016), *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*, Versoix, Icrc, https://shop.icrc.org/autonomous-weapon-systems-implications-of-increasing-autonomy-in-the-critical-functions-of-weapons.html (last accessed on 12th December 2022).

Itu (2005), *Wsis Outcome Documents: Geneva 2003-Tunis 2005*, Geneva, Itu, https://www.itu.int/net/wsis/outcome/booklet.pdf (last accessed on 5th December 2022).

Itu (2009), *Recommendation Itu-T X.1205: Overview of Cybersecurity*, Geneva, Itu, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items (last accessed on 5th December 2022).

Itu-T (2015), *Cybersecurity, Data Protection and Cyber Resilience in Smart Sustainable Cities*, Geneva, Itu, https://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/website/web-fg-ssc-0090-r7-technical_report_on_ICT_infrastructure_for_resilience_security.doc (last accessed on 5th December 2022).

Karns, M.P., Mingst, K.A. and Stiles, K.W. (2015), *International Organizations: The Politics and Processes of Global Governance*, Boulder, Lynne Rienner Publishers.

Keohane, R.O. (1984), *After Hegemony: Cooperation and Discord in the World Political Economy*, Princeton, Princeton University Press.

Keohane, R.O. (1989), *International Institutions and State Power: Essays in International Relations Theory*, New York, Routledge.

Keohane, R.O. (1993), *The Diplomacy of Structural Change: Multilateral Institutions and Stat*, in H. Haftendorn (ed.), *America and Europe in an Era of Change*, New York, Routledge, pp. 43-61.

Kirchner, E.J. and Dominguez, R. (2011), *The Security Governance of Regional Organizations*, Oxon, Routledge.

Majone, G. (1997), *From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance*, in «Journal of Public Policy», 17(2), pp. 139-167.

Mearsheimer, J.J. (1994), *The False Promise of International Institutions*, in «International Security», 19(3), pp. 5-49.

Mueller, M. (2010), *Networks and States: The Global Politics of Internet Governance*, Cambridge, Mit Press.

Mueller, M. (2017), *Is Cybersecurity Eating Internet Governance? Causes and Consequences of Alternative Framings*, in «Digital Policy, Regulation and Governance», 19(6), pp. 415-428.

Nato (1995), *Standardization Agreement on the Determination of the Classification of Military Ammunition and Explosives, Brussels*, Nato, https://www.difesa.it/Amministrazionetrasparente/segredifesa/terrarm/Documents/4123eed03a1.pdf (last accessed on 12th December 2022).

Nato (2022), *Arms Control, Disarmament and Non-Proliferation in Nato*, Nato, https://www.nato.int/cps/en/natohq/topics_48895.htm (last accessed on 12th December 2022).

Nato Rto (2007), *Uninhabited Military Vehicles (Umvs): Human Factors Issues in Augmenting the Force*, Brussels, Nato, https://www.sto.nato.int/publications/STO%20Technical%20Reports/RTO-TR-HFM-078/$$TR-HFM-078-ALL.pdf (last accessed on 12th December 2022).

Nicolson, H. (1942), *Diplomacy*, Oxford, Oxford University Press.

Oas (1997), *Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms*, Ammunition, Explosives, and Other Related Materials (A-

63), Washington D.C., OAS, https://www.oas.org/en/sla/dil/inter_american_treaties_A-63_illicit_manufacturing_trafficking_firearms_ammunition_explosives.asp (last accessed on 12th December 2022).

Oau (2009), *African Nuclear Weapon Free Zone Treaty (Treaty of Pelindaba)*, Cairo, Au, https://treaties.unoda.org/t/pelindaba (last accessed on 12th December 2022).

Opanal (1967), *Text of the Treaty of Tlatelolco*, Mexico City, Opanal, https://www.opanal.org/en/text-of-the-treaty-of-tlatelolco/ (last accessed on 12th December 2022).

Osce (1990), *Treaty on Conventional Armed Forces in Europe*, Paris, Osce, https://www.osce.org/files/f/documents/4/9/14087.pdf (last accessed on 12th December 2022).

Osce (1992), *Treaty on Open Skies, Helsinki*, Osce, https://www.osce.org/files/f/documents/1/5/14127.pdf (last accessed on 12th December 2022).

Osce (2011), *Vienna Document on Confidence and Security-Building Measures*, Vienna, Osce, https://www.osce.org/files/f/documents/a/4/86597.pdf (last accessed on 12th December 2022).

Paris, R. (2004), *At War's End: Building Peace after Civil Conflict*, Cambridge, Cambridge University Press.

Permanent Council Of The Oas (2016), *Consolidated List of Confidence and Security-Building Measures for Reporting According to Oas Resolutions*, Oas, http://scm.oas.org/IDMS/Redirectpage.aspx?class=CP/CSH&classNum=1043&lang=e (last accessed on 12th December 2022).

Petersen, K.L. (2016), *Risk and Security*, in M. Cavelty Dunn and T. Balzacq (eds.), *Routledge Handbook of Security Studies*, Oxon, Routledge, para. 11.

Rid, T. (2012), *Cyber War Will Not Take Place*, in «Journal of Strategic Studies», 35(1), pp. 5-32.

Rose, A. and Liao, S.Y. (2005), *Modeling Regional Economic Resilience to Disasters: A Computable General Equilibrium Analysis of Water Service Disruptions*, in «Journal of Regional Science», 45(1), pp. 75-112.

Rosenau, J.N. and Czempiel, E. (eds.) (1992), *Governance without Government: Order and Change in World Politics*, Cambridge, Cambridge University Press.

Ruggie, J. G. (1992), *Multilateralism: The Anatomy of an Institution*, in «International Organization», 46(3), pp. 561-598.

Russian Federation (1998), *Developments in the Field of Information and Telecommunications in the Context of International Security*, New York, Un, https://digitallibrary.un.org/record/263069 (last accessed on 11th December 2022).

Schmitt, O. (2016), *International Sanctions*, in M. Cavelty Dunn and T. Balzacq (eds.), *Routledge Handbook of Security Studies*, Oxon, Routledge, para. 33.

Sipri (n.d.), *Arms Embargoes*, Sipri, https://www.sipri.org/databases/embargoes (last accessed on 12th December 2022).

Tiirmaa-Klaar, H. (2016), *Building National Cyber Resilience and Protecting Critical Information Infrastructure*, in «Journal of Cyber Policy», 1(1), pp. 94-106.

Treaty on a Nuclear-Weapon-Free Zone in Central Asia (Canwfz) (2009), *Semipalatinsk*, Unoda, https://treaties.unoda.org/t/canwfz (last accessed on 12th December 2022).

Un (1945), *Chapter VIII: Regional Arrangements (Articles 52-54)*, San Francisco, Un, https://www.un.org/en/about-us/un-charter/chapter-8 (last accessed on 11th December 2022).

Un (1945a), *Chapter VI: Pacific Settlement of Disputes* (Articles 33-38), San Francisco, Un, https://www.un.org/en/about-us/un-charter/chapter-6 (last accessed on 11th December 2022).

Un (1945b), *Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression* (Articles 39-51), San Francisco, Un, https://www.un.org/en/about-us/un-charter/chapter-7 (last accessed on 11th December 2022).

Un (1945c), *Chapter I: Purposes and Principles (Articles 1-2)*, San Francisco, Un, https://www.un.org/en/about-us/un-charter/chapter-1 (last accessed on 11th December 2022).

Un (2001), *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, Geneva, Un, https://geneva-s3.unoda.org/static-unoda-site/pages/templates/the-convention-on-certain-conventional-weapons/CCW%2Btext.pdf (last accessed on 12th December 2022).

Un (2005), *International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons*, Unoda, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/ITI_English.pdf (last accessed on 12th December 2022).

Un (2014), *The Arms Trade Treaty*, New York, Un, https://thearmstradetreaty.org/hyper-images/file/ATT_English/ATT_English.pdf?templateId=137253 (last accessed on 12th December 2022).

Un (2019), *Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, Geneva, Un, https://undocs.org/CCW/MSP/2019/9 (last accessed on 12th December 2022).

Un Disarmament Commission (1988), *Special Report of the Disarmament Commission to the General Assembly on its Third Special Session devoted to Disarmament*, Unga, https://s3.amazonaws.com/unoda-web/documents/library/AS-15_3.pdf (last accessed on 12th December 2022).

Unga (1946). *Establishment of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy*, New York, Un, https://digitallibrary.un.org/record/209570?ln=en (last accessed on 11th December 2022).

Unga (2001), *Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, Supplementing the United Nations Convention against Transnational Organized Crime*, Un, http://www.unodc.org/

documents/treaties/UNTOC/Publications/A-RES%2055-255/55r255e.pdf (last accessed on 11th December 2022).

Unga (2002), *Combating the Criminal Misuse of Information Technologies*, New York, Un, https://digitallibrary.un.org/record/454952 (last accessed on 11th December 2022).

Unga (2006), *Developments in the Field of Information and Telecommunications in the Context of International Security*, New York, Un, https://digitallibrary.un.org/record/588209 (last accessed on 11th December 2022).

Unga (2011), *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, Un, https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/Res/65/230&Lang=E (last accessed on 11th December 2022).

Unga (2014), *Developments in the Field of Information and Telecommunications in the Context of International Security*, Un, https://digitallibrary.un.org/record/785132 (last accessed on 11th December 2022).

Unga (2015), *Report of the Secretary General on the Developments in the Field of Information and Telecommunications in the Context of International Security*, Un, https://digitallibrary.un.org/record/799853 (last accessed on 8th December 2022).

Unga (2019a), *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, Un, https://digitallibrary.un.org/record/1658328 (last accessed on 8th December 2022).

Unga (2019b), *Objective Information on Military Matters, Including Transparency of Military Expenditures*, Un, https://undocs.org/en/A/res/74/24 (last accessed on 11th December 2022).

Unga (2020), *Countering the Use of Information and Communications Technologies for Criminal Purposes*, Un, https://digitallibrary.un.org/record/3831879?ln=en (last accessed on 11th December 2022).

Un Gge (2013), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Un, https://digitallibrary.un.org/record/753055 (last accessed on 11th December 2022).

Un Gge (2022), *Report of the 2022 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, Geneva, Un, https://documents.unoda.org/wp-content/uploads/2022/08/CCW-GGE.1-2022-CRP.1-Rev.1-As-Adopted-on-20220729.pdf (last accessed on 12th December 2022).

Unidir (2014), *Framing Discussions on the Weaponization of Increasingly Autonomous Technologies*, Geneva, Un, https://unidir.org/publication/framing-discussions-weaponization-increasingly-autonomous-technologies (last accessed on 11th December 2022).

Unidir (2019), *The Role of Regional Organizations in Strengthening Cybersecurity and Stability*, Geneva, Un, https://unidir.org/publication/role-regional-organizations-strengthening-cybersecurity-and-stability (last accessed on 11th December 2022).

Unoda (2018), Securing Our Common Future: An Agenda for Disarmament, New York, Un, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf#view=Fit (last accessed on 11th December 2022).

Unroca (n.d.), *Roca (United Nations Register of Conventional Arms)*, Un, https://www.unroca.org/ (last accessed on 12th December 2022).

Unsc (2006), *Report by the Secretary General on regional-global security partnership: Challenges and opportunities*, Un, https://digitallibrary.un.org/record/581579?ln=en (last accessed on 11th December 2022).

Unsc (2015), *Resolution 2231*, Un, http://unscr.com/en/resolutions/doc/2331 (last accessed on 11th December 2022).

Waldrop, M. (2015), *Darpa and the Internet Revolution*, Darpa, https://www.darpa.mil/attachments/(2O15)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20(Approved).pdf (last accessed on 11th December 2022).

Walt, S.M. (1991), *The Renaissance of Security Studies*, in «International Studies Quarterly», 35(2), pp. 211-239.

Waltz, K.N. (1979), *Theory of International Politics*, Long Grove, Waveland Press.