Critical Information Infrastructure Protection: Between Cybersecurity and Policymaking

Anna Pagnacco [1,2,3]

[1] *Scuola Superiore Sant'Anna, Pisa, Italy*
[2] *Center for Cyber-Security and International Relation Studies (CCSIRS) – Università di Firenze, Firenze, Italy*
[3] *Laboratorio Nazionale Cybersecurity – CINI, Roma, Italy*

Abstract

The concept of Critical Information Infrastructure Protection (CIIP) is intrinsically interdisciplinary, as it depends on the development of informed estimates of potential threats, the individuation of appropriate responses and preventative measures and finally the proposal, application, and execution of relevant strategies. This poses the challenge of managing a field where regulation and cybersecurity collide, as the critical nature of the goods and services depending on CII's correct and uninterrupted functioning force policymakers to intervene in an environment shaped by the issues and assumptions typical of cyberspace.

In espousing this view, this paper seeks to explore the challenges arising from the intersection of these two perspectives, focusing first on a broad overview of CIIP's links with policymaking and cybersecurity and then mapping the reciprocal influence CII and selected geopolitical elements exert on each other at an international level. This leads to a reflection on potential ways to better integrate relevant perspectives on CIIP at the policy level.

Keywords

Critical Information Infrastructure Protection (CIIP), Critical Information Infrastructure, Policymaking, Cybersecurity, Physical Layer of Cyberspace, International Relations, Geopolitics

1. Introduction. Cybersecurity as a Priority

In light of recent events, for public perception and expert forecasting alike, cyber risk has been dwarfed by biological and environmental threats, both in terms of likelihood and potential damage [1]. Indeed, COVID-19 has doubtlessly changed the world's relationship with consumer technology, drastically accelerating a series of long-standing trends in tech adoption and development: the forced transition to "smart working" practices strongly incentivized workflow digitization [2], successfully phasing out physical processes [3] unless absolutely necessary. Commercial practices have been heavily impacted [4], further accelerating the digital revolution in consumer behaviour [5] [6]. Raising issues related to Critical Information Infrastructure (CII) is therefore far from untimely, as the pandemic has only furthered the world's reliance on their uninterrupted functioning [7].

At the policy level, the push to digitally transition has not stopped, as is highlighted by the existence of measures such as European programs specifically aimed at helping to digitize SMEs [8] and of dedicated national political authorities, such as the *Ministero per l'Innovazione tecnologica e la Digitalizzazione* in Italy. However, successful policymaking in cyberspace requires more than just adequate funding, as the field confronts lawmakers with complex challenges in terms of anonymity, asymmetry, democratization of violence and instability [9]. In the face of such dire circumstances, the fundamental policy procedure of setting measurable objectives and implementing a feedback loop on their effectiveness [10] does not easily apply, since all threat models are but informed estimates [11].

ITASEC – Italian Conference of Cybersecurity, April 7–9, 2021, Roma, Italy
EMAIL: a.pagnacco@santannapisa.it
ORCID: 0000-0002-2329-2793

However, while unaccounted-for vulnerabilities can vanquish all protective effort, focusing on worst-case scenarios does not guarantee an efficient allocation of resources either [12]. The fact that it is impossible to completely secure any given system might make it harder to justify increasingly harsher protective measures – both in terms of user friction and of the expenses needed to adequately put them in place – only to achieve what may be perceived as a slight or incremental improvement in overall security.

The infrastructural function of cyberspace cannot be dismissed as a merely technical matter, as it both follows geopolitical criteria and lays the foundation for "fifth dimensional" international relations [13]. Critical Information Infrastructure Protection (CIIP) is therefore an intrinsically interdisciplinary policy field, as it depends on the development of informed estimates of potential threats, the individuation of appropriate responses and preventative measures and finally the proposal, application, and execution of relevant strategies. This poses the challenge of managing a field where traditional regulatory practices and cybersecurity collide, as the critical nature of the goods and services depending on CII's correct and uninterrupted functioning force policymakers to interact with an environment shaped by the issues and assumptions typical of cybersecurity. Unfortunately, public attention to long-term security risks is often surpassed by more immediate concerns, often connected to infrastructure reliability and availability [14]. The lack of urgency in the adoption of long-term strategic measures in CIIP is therefore not an indication of structural irrelevance: a proper level of information security is critical to allow for a robust expansion of internet-based services [15] and even to adequately manage some logistic sides of the COVID crisis [16].

Not unlike most cybersecurity problems, drawing attention to it can both advance and complicate the field's overall situation. On the one hand, increasing the general public's awareness of CIIP can have relevant positive consequences; and identifying vulnerabilities with the aim of proposing or soliciting solutions is indeed a legitimate research exercise that can raise awareness of existing problems. On the other hand, this practice might increase the risk of exposing CII to malicious exploitation, which is particularly worrying with regards to vulnerable systems that might not be easily fixed [14] – so much so that it is possible to hypothesize that a Coordinated Vulnerability Disclosure (CVD) framework might apply. It is therefore important to highlight the qualitative nature of this study, which refrains from any analysis of specific systems' vulnerabilities, choosing to focus on strategic evaluations of geopolitical trends and international regulation instead.

2. Critical Information Infrastructure Protection (CIIP): Cybersecurity and Policy

2.1. Defining Critical Information Infrastructure

Even though literature has not converged on a single definition of CII yet, it is necessary to adopt a working definition of the concept, nonetheless. As a starting point, we can consider CIIs all *those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy* [17]. This broad ENISA definition is substantially aligned with the European Union's position in favour of recognizing the increasingly critical nature of ICTs and of cyberspace [15] and it gives rise to a potential subdivision of CIIs in two broad categories.

The first category includes the physical components of cyberspace, with special emphasis on the global network of undersea cables that enable the existence of cyberspace itself [18]: its large extension and submarine positioning, as well as the presence of geographical bottlenecks [19], make it a difficult target for protection as well as a strategically relevant factor in international politics [20]. As the most tangible of CIIs, physically connecting different locations, it is also the most conceptually similar to traditional critical infrastructure, being vulnerable to a number of physical attacks and damage factors. It is fundamental to draw attention to this specific infrastructure since the cutting edge of innovation is mostly focused on developing immaterial services – as demonstrated by the exceptional developments in "cloud-"based solutions as well as Software as a Service (SaaS) business models. On the matter of connectivity, the industry's emphasis on wireless mobile technology, best

exemplified by the high salience of 5G networks in public discourse, risks overshadowing the fundamental relevance of cable infrastructure that underlies it all.

The second category of CII, according to Luiijf [17], includes all Information and Communication Technologies (ICTs) that *monitor, control, or interact with other CI and our physical world*. The critical nature of physical information infrastructure is therefore granted following the complete reliance of critical sectors on its steady, uninterrupted functioning. The most prominent example of such an infrastructure is the Internet, as a large-scale network which depends on the physical layer. While it does not necessarily constitute a critical infrastructure in and of itself, it has grown to be fundamental for most functions in a digitized society, including the workings of "traditional" critical infrastructures such as banking and finance circuits, global supply chains and medical facilities [21]. This definition allows for a greater extension of this concept, which can be easily said to include all technical devices whose malfunctioning would impact any critical infrastructure. Systems that rely on Internet connectivity, with applications such as online Industrial Control Systems (ICS) for critical industries and connected devices with control over physical applications [22], are therefore also CII.

2.2. CIIP and cybersecurity

It must be noted that in the field of CIIP most fundamental assumptions from cybersecurity hold true. Unlike what happens with most policy fields, it is impossible to even theorize a complete success in protecting cyberspace*:* in cybersecurity, it is posited that *any safety margin will, by necessity, be finite and one cannot anticipate any and all contingencies that may either be wholly unanticipated or have a very low probability of occurrence* [14].

Another fundamental peculiarity of cyberspace that also applies to critical infrastructure protection [23] is the emphasis on a "weakest link" approach [24]. Isolated security practices, however sophisticated or expensive, are not conducive to greater overall security compared to best practices implemented consistently across the board. On the contrary, the friction created by strict but inconsistent measures may well create the illusion of strong overall security, potentially leading users to place an excessive amount of trust in vulnerable systems [25]. At a policy level, however, zero trust policies are especially hard to implement: they increase friction and run counter to intuitive human thinking.

The framing of cyberspace as a critical infrastructure also creates a situation of convergence between technical or Information Security and National Security [26], which must be properly managed in order to account for the methodological differences between the two fields. Protection of cyberspace and its infrastructures therefore requires an interdisciplinary approach, rewarded in practice but not in theory as it might mean a multiplication of relevant events, definitions, and actors. However, this complexity can better account for deliberate malfunctions that escape probabilistic considerations, going beyond technical solutions such as increased reliability and fault tolerance. Security must be based not only on technical convergence [27], but on an "all-hazards approach" that "includes accidents, natural hazards as well as deliberate attacks", accounting for both the intention and the capability – means and motive – of potential attackers [28].

In this light, CIIP can be understood as the natural extension of cyberspace protection to the physical layer: all cybersecurity efforts, even the most up-to-date, consistent, and sophisticated, could be rendered useless if the physical layer on which information flows is not properly secured and accounted for.

2.3. The political relevance of CIIP

The protection of critical infrastructure has always been a subject of attention by political authorities; CIIP is a matter of sovereignty, as it links cyberspace to geopolitical reality both structurally [29] and functionally [30]. However, issues such as the private ownership of CII, their apparently non-essential nature and the scarce attention that is generally devoted to them appear to be relegating CIIP less in the realm of policy and more towards strictly technical regulation [31]. CIIP definitely belongs in the former for at least three main reasons: prioritization, public coordination and national security relevance.

Even the most technically informed decisionmaker cannot merely execute experts' recommendations, because even assuming that their position can be truly apolitical, unbiased, comprehensive, and objective – which is almost never the case [32] – it would be impossible to enact all suggested policy measures with the same urgency. Since it is impossible to completely secure everything, any choice of protection priorities is then inherently political [33]. Furthermore, the fundamental process of prioritization of some issues over others in the policymaker's agenda must also consider the presence of external elements such as economic matters, funding procedures and international politics, as well as instances introduced by other stakeholders in the public discourse [34], particularly in democratic contexts.

A plurality of public, private, and mixed actors are involved in CII ownership and maintenance [35]. Management of this type of critical infrastructure is as urgent as it is complex, since it must reconcile citizens' rights and expectations regarding uninterrupted and reliable functioning with the fast pace of a dynamic technological market, where components, procedures, and best practices might quickly become outdated. Coordination of such a complex ecosystem, especially in light of the relevant consequences in case of failure, should naturally fall under the purview of competent public authorities.

Lastly, the framing of defensive actions in cyberspace as "fifth domain" military operations [36] vouches for the validity of a National Security approach to cybersecurity and CIIP [37]. It is only natural that the infrastructural components of what has been established as a valid domain of legitimate nation-state action fall within the purview of national security policy. While this has been explicitly recognized for "ICT and Internet security" [15], one must also acknowledge that the targeting of CII in order to indirectly harm other objectives can turn them into weapons in their own right [17]. To further clarify the extent to which the inner workings of contemporary society are vulnerable, the European Parliament itself recognized CII as critical for eleven sectors: energy, the nuclear industry, ICT, water, food, health, the financial sector, transportation, the chemical industry, the space industry, and research facilities [21]. This becomes even more obvious when taking into consideration the role of interconnection between elements of CIs and various CIs, which can amplify the severity of failures and further jeopardize the recovery process after any disruptive event [14].

3. A Geopolitical Perspective on CIIP

3.1. Infrastructure ownership

Infrastructure ownership is a critical point of intersection between cybersecurity concerns and traditional geopolitics. This can be seen specifically with regards to both the frequently private or mixed ownership of critical infrastructure and the political implications of foreign infrastructure ownership.

The European Parliament recognizes that *the private sector remains the primary investor in, and owner and manager of, information security products, services, applications and infrastructure*, underlining the need for the political authority to outline appropriate coordination strategies [15] and tools such as Public-Private information sharing arrangements [26]. On the one hand, it is often hard to tie relevant actors to stable geopolitical entities, as they span between public, private, and mixed ownership forms; the presence of transnational partnerships and conglomerates [38] strongly challenges the usefulness of locally implemented policies. On the other hand, supposedly private actors are increasingly offering infrastructural services [39], blurring the line between their market-driven agenda and nation-state policies, either for government steering and support [40] or through massive institutional lobbying [41].

Infrastructure ownership can also translate to political pressure. China's Belt and Road Initiative (BRI) is a prime example of this, as it couples massive capital availability with opaque funding management [42]. Even assuming the absence of explicit political conditions and a positive motivation derived from a willingness to advance more fragile projects and economic systems [43], this system can lead to riskier investments for borrower countries – exposing them to potential debt distress [44] – as well as the funding of anti-democratic practices. Even though the framing of the BRI as "debt trap diplomacy" is contested [45], a strong foreign presence in infrastructure financing and ownership is bound to imply some degree of influence, even just by exerting soft power by creating or

withdrawing positive interventions in terms of local economy growth and security [46]. The same dynamics are at play with the Digital Silk Road, BRI's digital division, which supports the funding of CIIs such as undersea communication cables [47] and other telecommunications infrastructures [48], including technology used for innovative applications such as smart cities [49].

3.2. Threats to CII: supply chains, cyberattacks, physical attacks

Cyberspace is a hybrid landscape comprised of three "layers": physical, logical, and social [9]. Vulnerabilities can occur on all three; therefore, it is important not to focus exclusively on the part of cyberspace made up of code, but also on the interplay between code and the infrastructure that allows it to run. Supply chains are one of the steps where security concerns meet with economic preoccupations. Political instances can influence both the secure availability of materials – as happens with the semi-natural Chinese monopoly on rare earths [51] – and the cybersecurity of fundamental components in technological supply chains. At the logic level, the recent Solarwinds hack [51] and Ripple20 disclosure [52] have recently demonstrated how far-reaching the consequences of single attack can be when it is positioned at the beginning rather than at the end of a software supply chain.

The same holds true for CII: the reliability of the physical layer is the first step to enable all successive layers of cyberspace to be reliable themselves [53]. Procedures that compromise the physical layer of CII, such as the hypothesis of hardware components tampering, have been raised not just as Proof-of-Concept experiments [54], but also in the vastly disputed report alleging Chinese tampering on Supermicro systems [55], which still stands as a relevant example of the challenges brought up by the convergence of geopolitical tensions and cybersecurity concerns. The anonymity of all cited sources and the lack of technical detail are a great reminder of just how challenging attribution can be, especially with regards to linking operations to politically motivated actors. While the US intelligence community never confirmed the allegations [56], documents leaked by Edward Snowden proved the existence of NSA procedures compromising hardware during the shipping process and components designed to be implanted into various types of devices [54], catapulting such threats in the realm of concrete possibility.

In fact, just as vulnerabilities in code, CII have already been weaponized. Much like the Internet itself, cyberspace weaponization originated in the US, with the first test ("Aurora") demonstrating the irreversible destruction of a power generator via code [57]. While Stuxnet allowed the USA to target a traditionally off-limits critical infrastructure, it has vastly reduced the country's moral high ground in the conduct of "cyberwarfare", starting a cascade effect that has brought all major cyber-powers to use all means as long as plausible deniability allows it [58]. The Russian Federation is one of the main offenders, as it has been linked to a series of disruptive actions towards critical infrastructures in Estonia around 2007 and in Ukraine between 2015 and 2017 [57]. In this case, the massive use of offensive cyber capabilities allows for a compensation of the reduced traditional military power [59], asymmetrically projecting power on the international scene [60] without any international accountability for civilian collateral damage [61].

The disruption of CIIs can happen via cyberattack [62], but their double, digital and physical nature means that kinetic attacks are possible, too. While "bombing the Internet" is not a viable solution – as it would require immense effort to exceed local disruptions [63] by targeting most nodes in its distributed network [64] – and physical disruption of ICSs is impractical, as the level of access it requires is the same needed to physically disrupt the productive processes themselves, the same cannot be said for other backbone technology such as submarine cable networks, whose extensive length, undersea collocation and thin diameter make for perfect physical operations targets [65] [66].

3.3. An opening for regulation?

Even though the elements outlined paint the picture of a field of great interest for policymakers, this complex international scenario does not facilitate the creation of a comprehensive protection scheme for information systems aimed at systematically covering all their vulnerable points. Indeed, it is not inappropriate to wonder whether interest for any such protective strategy exists at all. It is especially hard to envision the enforcement of a global regulatory protection scheme given that all

major cyber-powers would rather be able to fully dispose of their offensive capabilities in cyberspace, since traditional, well-understood mechanisms and theories on reactions to and deterrence of malicious activity apply inconsistently at best [14]. Nation-state actors are therefore either too small to create sufficient critical mass in policy settings or big enough to benefit from their independence in this vastly underregulated landscape [65].

Signals Intelligence (SIGINT) gathering operations, for instance, far from being limited to software-level eavesdropping, also happen directly at the physical communications layer [67] [68], with undersea fiber optic cables taking center stage and lacking a coherent protection framework [69]. The potential regulatory role of International Organizations and *fora* such as NATO is greatly reduced by the existence of more restricted partnerships, such as the Five Eyes information sharing system, which includes agreements on CIIP [70] [71]. It is important to note that, although EU member states such as Germany and France have expressed interest in joining, no European country is party to this closer intelligence collaboration, although major European countries can be found within slightly wider partnerships such as the so-called "Nine Eyes" and "Fourteen Eyes" (SSEUR) [72]. Recent talks of a Japan addition to the core alliance [73] demonstrate that, rather than just following historical proximity, these partnerships are first and foremost rooted in ever-evolving geopolitical dynamics.

The EU itself *has repeatedly insisted on applying high standards for data privacy and data protection, net neutrality, and intellectual property rights protection*, going so far as taking steps to establish a European CIIP framework as a direct response to *cyberattacks against the information infrastructure of EU institutions, industry and Member States* [15]. These actions are seen as complementary to the efforts against terrorism, cybercrime, and the developments in information security [74]. While the EU highlights an openness to full cooperation with international initiatives in this area, the recognition of political, economic and information elements throughout relevant official documents shows that it is ready to uphold stricter terms in CIIP, fully grasping the relevance of the connections with cybersecurity and defence and acknowledging that disruptive threats to the functioning of civilian CII are no longer just hypothetical in nature [26].

The EU officially recognizes *ICT and internet security* as *a comprehensive concept with a global impact on economic, social, technological, and military aspects, demanding a clear definition and differentiation of responsibilities as well as a robust international cooperation mechanism* [15]. However, implementing said international cooperation is challenging, to the point it is not clear whether such a project would ever succeed. Even though some scenarios might seem excessively catastrophic, their likelihood keeps increasing as long as this unstable situation is protracted. In conjunction with potential symmetrical conflicts, the ability to attack CIIPs would immediately constitute one of the primary means of impacting civilian structures and livelihood. In recognition of this threat and after much debate, NATO has recently decided Article 5 applies in response to cyberattacks as well [76], taking a fundamental step forward towards cyberspace stabilization. Unfortunately, that barely settles all questions raised by this approach to the relationship between warfare and cyberspace. Is kinetic action ever a commensurate response to a cyberattack? If so, how is response proportionality measured? What level of attribution certainty must be obtained before responding? What are the terms of responsibility for nation-states denying their involvement? Such questions have already begun to be explored, but they are still far from gathering significant consensus, as relevant considerations are constantly evolving and therefore tentative at best [76].

As for what concerns CIIP specifically, a significant increase in the amount of such regulation at a regional level would create fragmentation, paradoxically opposing the achievement of the proposed aim by limiting citizens' potential use of cyberspace. For instance, it is unlikely that other countries would apply stricter EU CIIP norms, effectively limiting their scope to European actors. Trying to force international compliance by conditioning access to the European Digital Market would be extremely risky: in such a scenario the withdrawal of international noncompliant players would likely cause the EU to be unintentionally cut off from the rest of the world, as infrastructure-level global interconnectivity is intrinsic to the Internet's functioning. Therefore, local CIIP developments must be encouraged and welcomed, but in order to minimize the collateral damage they could pose to international equilibrium, they should always be clearly positioned in a local defensive perspective, since international collaboration is hampered by the lack of shared limitations to offensive action.

4. Conclusions

International norms can only exert a limited amount of deterrence in cyberspace, both because they oftentimes only apply *ex post*, and because of the chronic difficulties in the attribution process. Moreover, some of the aforementioned scenarios involving attacks on CII were foreseen but explicitly not criminalized. For instance, while the 1884 Convention for the Protection of Submarine Telegraph Cables penalizes the intentional cutting of submarine cables, Article 15 allows that the Convention's norms do not apply in wartime. This means that, except for selected parties bound by specific international agreements, it was explicitly chosen not to declare it illegal to engage in so-called "cable wars", such as those pioneered by the UK in World War I [77]. To say that reliance on the Internet has increased since then would be an understatement: rather than just delaying or intercepting strategic communications, nowadays this tactic would prove incredibly consequential, significantly hampering civilian life. Such predictions, however, suffer from the same issue that plagues CIIP as a field: while their relevance is perfectly logical and easily demonstrated, they are often overlooked in favour of shorter-term policy goals or shallower but more tangible infrastructural issues.

Securing vulnerable infrastructures is a never-ending optimization process that requires correct policy prioritization of CII issues with respect to more flashy interventions. This can only be achieved by combining a horizontal approach of "contamination" between disciplines and a vertical approach of "involvement" of all societal components involved. As for what concerns the horizontal dimension, the field of CIIP can, by nature, only develop through interdisciplinarity: it is important to intersect perspectives from scholars in both technical fields and the Social Sciences – namely Political Science, International and Comparative Law and International Relations – but also to consider and evaluate relevant experiences and observations from non-academic personnel, since, as this paper has hopefully shown, this area is strongly shaped by processes and assumptions typical of cyberspace as well as by Defence optics, both traditional and contemporary. With respect to the vertical dimension, policymakers must foster fruitful exchanges between bearers of diverse expertise at all levels of the political process, from policy analysis to policymaking. In order to achieve this, it is fundamental to raise awareness and create spaces of collaboration between policymakers, industry stakeholders and academia. Finally, technical and scholarly expertise cannot be confined in a bubble of niche theories and developments; on the contrary, it must be widely shared with both policymakers and the general public, generating a virtuous cycle of attention and public pressure aimed at better CII protection.

On the international stage, as for now, pushing for increased local regulation while encouraging the potential formation of an international consensus still appears to be the best solution. Even though regional policy action inevitably breeds fragmentation, running counter to CIIP's goal of guaranteeing access to cyberspace as well as digital goods and services, CII vulnerabilities are not bound to disappear for lack of attention by political authorities and the wider public. A higher level of protection in a single region, such as the EU, should therefore be balanced with an active search for an agreement to consecrate the widest possible consensus. Starting first with a minimum common denominator, we should ideally go on to establish a diversified but cohesive global framework, slowly but steadily reducing impunity for attacks on CII. In the meantime, it is fundamental that policymakers coordinate CIIP efforts while strategically evaluating critical sectors' dependence on CIIs. Far from taking a luddite stand, the case for CIIP proves that only strong security will allow to fully reap the benefits of new ICT developments [15].

5. References

[1] World Economic Forum, *The Global Risks Report 2020*, 2020. URL: https://www.weforum.org/reports/the-global-risks-report-2020

[2] Deloitte Legal, *Accelerate digitization to increase resilience. A global COVID-19 response for legal leaders*, 2020. URL: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Legal/dttl-legal-covid-respond-legal-digitization.pdf

[3] Berti, M. (2020, 09 30). Dallo 0,8% ai potenziali 8 milioni di smart worker: così il COVID ha cambiato la geografia del lavoro. *ANSA.it*. URL:

https://www.ansa.it/canale_lifestyle/notizie/societa_diritti/2020/09/29/dallo-08-ai-potenziali-8-milioni-di-smart-worker-cosi-il-covid-ha-cambiato-la-geografia-del-lavoro_4e756577-77b4-4496-bcd1-e953f2493021.html

[4] UNCTAD. (2020, 10 08). *COVID-19 has changed online shopping forever, survey shows.* URL: UNCTAD - United Nations Conference on Trade and Development: https://unctad.org/news/covid-19-has-changed-online-shopping-forever-survey-shows

[5] OECD. (2020, 10 07). *OECD Policy Responses to Coronavirus (COVID-19): E-commerce in the time of COVID-19.* URL: OECD.org: http://www.oecd.org/coronavirus/policy-responses/e-commerce-in-the-time-of-covid-19-3a2b78e8/

[6] UNCTAD, Netcom Suisse, *COVID-19 and E-commerce. Findings from a survey of online consumers in 9 countries*, 2020. URL: https://unctad.org/system/files/official-document/dtlstictinf2020d1_en.pdf

[7] CISA. (2020, 04 08). *Alert (AA20-099A): COVID-19 Exploited by Malicious Cyber Actors.* URL: https://us-cert.cisa.gov/ncas/alerts/aa20-099a

[8] European Commission. (2020, 10 23). *European Digital Innovation Hubs in Digital Europe Programme.* URL: European Commission: https://ec.europa.eu/digital-single-market/en/european-digital-innovation-hubs-digital-europe-programme-0

[9] Martino, Luigi. "La quinta dimensione della conflittualità. L'ascesa del cyberspazio ei suoi effetti sulla politica internazionale." *Politica & Società* 7.1 (2018): 61-76.

[10] Howlett, Michael, Ishani Mukherjee, and Jun Jie Woo. "From tools to toolkits in policy design studies: The new design orientation towards policy formulation research." *Policy & Politics* 43.2 (2015): 291-311.

[11] OWASP, *Threat Modeling*. URL: https://owasp.org/www-community/Threat_Modeling

[12] Murray, Alan T., and Tony H. Grubesic. "Critical infrastructure protection: The vulnerability conundrum." *Telematics and informatics* 29.1 (2012): 56-65.

[13] Starosielski, Nicole. *The undersea network*. Duke University Press, 2015.

[14] Lopez, Javier, Roberto Setola, and Stephen D. Wolthusen. "Overview of critical information infrastructure protection." *Critical Infrastructure Protection*. Springer, Berlin, Heidelberg, 2012. 1-14.

[15] European Parliament, 2012. *European Parliament resolution of 12 June 2012 on critical information infrastructure protection - achievements and next steps towards global cyber-security [2011/2284(INI)]*. URL: https://www.europarl.europa.eu/doceo/document/TA-7-2012-0237_EN.pdf

[16] Columbus, L. (2021, 01 24). 10 Ways Covid-19 Vaccine Supply Chains Need To Be Protected By Cybersecurity. *Forbes.* URL: https://www.forbes.com/sites/louiscolumbus/2021/01/24/10-ways-covid-19-vaccine-supply-chains-need-to-be-protected-by-cybersecurity/

[17] Luiijf, Eric. "Understanding cyber threats and vulnerabilities." *Critical infrastructure protection* (2012): 52-67.

[18] Burnett, Douglas, Tara Davenport, and Robert Beckman. "Introduction. Why Submarine Cables?." *Submarine Cables*. Brill Nijhoff, 2014. 1-15.

[19] Coffey, Valerie. "Sea change: The challenges facing submarine optical communications." *Optics and Photonics News* 25.3 (2014): 26-33. URL: https://www.osapublishing.org/DirectPDFAccess/8E4F0F3A-2CA6-4870-A7AF2F17AF697CA1_281128/opn-25-3-26.pdf

[20] Fouquet, H. (2021, 03 05). China's 7,500-Mile Undersea Cable to Europe Fuels Internet Feud. *Bloomberg Businessweek*. URL: https://www.bloomberg.com/news/articles/2021-03-05/china-s-peace-cable-in-europe-raises-tensions-with-the-u-s

[21] Glorioso, Andrea, and Andrea Servida. "Infrastructure sectors and the information infrastructure." *Critical Infrastructure Protection*. Springer, Berlin, Heidelberg, 2012. 39-51.

[22] Alcaraz, Cristina, Gerardo Fernandez, and Fernando Carvajal. "Security aspects of SCADA and DCS environments." *Critical Infrastructure Protection*. Springer, Berlin, Heidelberg, 2012. 120-149.

[23] Brown, Gerald G., et al. "Analyzing the vulnerability of critical infrastructure to attack and planning defenses." *Emerging Theory, Methods, and Applications*. Informs, 2005. 102-123.

[24] Esteves, Jose, Elisabeth Ramalho, and Guillermo De Haro. "To improve cybersecurity, think like a hacker." *MIT Sloan Management Review* 58.3 (2017): 71.
[25] Kindervag, John, and S. Balaouras. "No more chewy centers: Introducing the zero trust model of information security." *Forrester Research* (2010): 3.
[26] Cavelty, Myriam Dunn, and Manuel Suter. "The art of CIIP strategy: tacking stock of content and processes." *Critical Infrastructure Protection*. Springer, Berlin, Heidelberg, 2012. 15-38.
[27] CISA, *Cybersecurity and physical security convergence*, 2021. URL: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20and%20Physical%20Security%20Convergence_508_01.05.2021.pdf
[28] Commission of the European Communities, 2005. *Glossary - Green paper on a european programme for critical infrastructure protection.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52005DC0576&from=EN
[29] Warf, Barney. "Alternative Geographies of Cyberspace." *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance* (2017): 147-64.
[30] Bambenek, J., Come la Russia proietta la sua potenza cibernetica. *LIMES - La rete a stelle e strisce*, 2018.
[31] Spadaro, I., & Pagnacco, A., Geostrategic value of submarine internet cables. *CCSIRS Policy Papers*, 2021. URL: https://www.cssii.unifi.it/upload/sub/Policy%20Paper/CCSIRS_Policy_Paper_February_2021.pdf
[32] Chung, Wonsuk, and Rick Harbaugh. "Biased recommendations from biased and unbiased experts." *Journal of Economics & Management Strategy* 28.3 (2019): 520-540.
[33] Walgrave, Stefaan, and Yves Dejaeghere. "Surviving information overload: How elite politicians select information." *Governance* 30.2 (2017): 229-244.
[34] Halpin, Darren R., Bert Fraussen, and Anthony J. Nownes. "The balancing act of establishing a policy agenda: Conceptualizing and measuring drivers of issue prioritization within interest groups." *Governance* 31.2 (2018): 215-237.
[35] Crain, J. K., Assessing resilience in the global undersea cable infrastructure, Master's Thesis, *Naval Postgraduate School, Monterey (CA)*, 2012. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a562772.pdf
[36] Welch, L., 2011. *Cyberspace - The Fifth Operational Domain.* IDA Research Notes - Challenges in Cyberspace. URL: https://www.ida.org/upload/research%20notes/researchnotessummer2011.pdf
[37] Dunn Cavelty, Myriam. "Cyber-Security". *The Routledge Handbook of New Security Studies* (2010): 154-162
[38] Green, Mick. "The Submarine Cable Industry: How Does It Work?." *Submarine cables*. Brill Nijhoff, 2014. 41-60.
[39] Reynolds, M. (2018, 07 26). Facebook and Google's race to connect the world is heating up. *WIRED*. URL: https://www.wired.co.uk/article/google-project-loon-balloon-facebook-aquila-internet-africa
[40] Hout, T., & Ghemawat, P. (2010, 12). China vs the World: Whose Technology Is It? *Harvard Business Review*. URL: https://hbr.org/2010/12/china-vs-the-world-whose-technology-is-it
[41] Romm, T. (2020, 01 22). Tech giants led by Amazon, Facebook and Google spent nearly half a billion on lobbying over the past decade, new data shows. *The Washington Post*. URL: https://www.washingtonpost.com/technology/2020/01/22/amazon-facebook-google-lobbying-2019/
[42] Crabtree, J. (2019, 04 26). China Needs to Make the Belt and Road Initiative More Transparent and Predictable. *Chatham House*. URL: https://www.chathamhouse.org/2019/04/china-needs-make-belt-and-road-initiative-more-transparent-and-predictable
[43] Ayodele, Thompson, and Olusegun Sotola. "China in Africa: An evaluation of Chinese investment." *Initiative for Public Policy Analysis* (2014): 1-20.
[44] Hurley, John, Scott Morris, and Gailyn Portelance. "Examining the debt implications of the Belt and Road Initiative from a policy perspective." *Journal of Infrastructure, Policy and Development* 3.1 (2019): 139-175.

[45] Brautigam, Deborah. "A critical look at Chinese 'debt-trap diplomacy': The rise of a meme." *Area Development and Policy* 5.1 (2020): 1-14.
[46] Jakimów, Małgorzata. "Desecuritisation as a soft power strategy: the Belt and Road Initiative, European fragmentation and China's normative influence in Central-Eastern Europe." *Asia Europe Journal* 17.4 (2019): 369-385.
[47] Zhu, Valerie. (2020, 01 25). Envisioning China's Digital Silk Road. *The Gate*, pp. http://uchicagogate.com/articles/2020/1/25/envisioning-chinas-digital-silk-road/.
[48] Kitson, A., & Liew, K. (2019, 11 14). China Doubles Down on Its Digital Silk Road. *Reconnecting Asia*. URL: https://reconnectingasia.csis.org/analysis/entries/china-doubles-down-its-digital-silk-road/
[49] Ekman, Alice, and Cristina de Esperanza Picardo. "Towards urban decoupling? China's smart city ambitions at the time of Covid-19." *European Union Institute for Security Studies, May* 14 (2020): 2020. URL: https://www.iss.europa.eu/content/towards-urban-decoupling-china%E2%80%99s-smart-city-ambitions-time-covid-19
[50] Hijazi, J., & Kennedy, J. (2020, 10 27). How the United States Handed China its Rare Earth Monopoly. *Foreign Policy*. URL: https://foreignpolicy.com/2020/10/27/how-the-united-states-handed-china-its-rare-earth-monopoly/
[51] Williams, J. (2020, 12 15). What You Need to Know About the SolarWinds Supply-Chain Attack. *SANS*. URL: https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/
[52] Oberman, S., Koi, M., & Schön, A., "Hacking the Supply Chain - The Ripple20 Vulnerabilities Haunt Hundreds of Millions of Critical Devices". *DEF CON 28 Safe Mode*, 2020.
[53] Bratton, B. H., *The stack: on software and sovereignty*, 2016, MIT press.
[54] Hudson, T. (2018). *Modchips of the State.* URL: CCC - Chaos Communications Congress: https://ftp.fau.de/cdn.media.ccc.de/congress/2018/h264-hd/35c3-9597-eng-deu-fra-Modchips_of_the_State_hd.mp4
[55] Robertson, J., & Riley, M. (2018, 10 04). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg Businessweek.* URL: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
[56] Wray, C. (2018, 10 10). *Homeland Security Threats.* URL: C-SPAN: https://www.c-span.org/video/?452548-1/secretary-nielsen-fbi-director-wray-testify-homeland-security-threats
[57] Greenberg, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Anchor, 2020.
[58] Zetter, Kim. *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Broadway books, 2014.
[59] Putin, Vladimir. Солдат есть звание высокое и почетное ('Soldier' is an honourable and respected rank). *Address to the Federal Assembly of the Russian Federation ("Krasnaya zvezda")*, 2006. URL: http://old.redstar.ru/2006/05/11_05/1_01.html
[60] Giles, Keir. "*Handbook of Russian Information Warfare.*" (2016). Rome: Nato Defense College - Fellowship Monograph.
[61] Wheeler, T. (2018, 09 12). In cyberwar there are no rules. *Foreign Policy*. URL: https://foreignpolicy.com./2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/
[62] Tabansky, Lior. "Critical Infrastructure Protection against cyber threats." *Military and Strategic Affairs* 3.2 (2011): 2. URL: https://i-hls.com/wp-content/uploads/2013/03/Critical-Infrastructure-Protection-against-Cyber-Threats-Lior.pdf
[63] Harris, S. (2020, 12 29). Nashville bombing is a potent reminder that communications systems remain at risk from attack. *The Washington Post*. URL: https://www.washingtonpost.com/national-security/nashville-bombing-is-a-potent-reminder-that-communications-systems-remain-at-risk-from-attack/2020/12/28/
[64] Cohen, Reuven, et al. "Resilience of the internet to random breakdowns." *The Structure and Dynamics of Networks*. Princeton University Press, 2011. 507-509.

[65] Aldrich, Richard J., and Athina Karatzogianni. "Postdigital war beneath the sea? The Stack's underwater cable insecurity." *Digital War* (2020): 1-7.
[66] Peach, S. S. (2017, 12 14). *Annual Chief of the Defence Staff Lecture 2017.* URL: Royal United Services Institute: https://rusi.org/sites/default/files/20171214-rusi-cds_annual_lecture-acm_peach.pdf
[67] Ball, J. (2013, 06 08). NSA's Prism surveillance program: how it works and what it can do. *The Guardian*. URL: https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google
[68] Timberg, C. (2013, 07 10). NSA slide shows surveillance of undersea cables. *The Washington Post*. URL: https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/
[69] Davenport, Tara. "Submarine cables, cybersecurity and international law: An intersectional analysis." *Cath. UJL & Tech* 24 (2015): 57.
[70] CISA. (n.d.). *International Critical Infrastructure Engagement.* URL: CISA.gov: https://www.cisa.gov/international-critical-infrastructure-engagement
[71] Critical 5. (2014). *Forging a Common Understanding for Critical Infrastructure - Shared Narrative.* URL: https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf
[72] Gallagher, R. (2018, 03 01). The powerful global spy alliance you never knew existed. *The Intercept*. URL: https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/
[73] Akita, H. (2020, 12 22). Pros and cons of a Six Eyes with Japan and allies. *NikkeiAsia*. URL: https://asia.nikkei.com/Spotlight/Comment/Pros-and-cons-of-a-Six-Eyes-with-Japan-and-allies
[74] European Commission. (2009). *Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
[75] Stoltenberg, J. (2019). NATO will defend itself. *Prospect - Cyber Resilience*, 4. URL: https://www.prospectmagazine.co.uk/content/uploads/2019/08/Cyber_Resilience_October2019.pdf
[76] Libicki, Martin C. "Correlations Between Cyberspace Attacks and Kinetic Attacks." *2020 12th International Conference on Cyber Conflict (CyCon)*. Vol. 1300. IEEE, 2020.
[77] Innovating in Combat. *From Australia to Zimmermann: A Brief History of Cable Telegraphy.* URL: University of Leeds - Museum of the History of Science, Oxford: https://blogs.mhs.ox.ac.uk/innovatingincombat/files/2013/03/Innovating-in-Combat-educational-resources-telegraph-cable-draft-1.pdf