KER KOREA EUROPE REVIEW
AN INTERDISCIPLINARY JOURNAL OF POLITICS, SOCIETY, AND ECONOMICS
ISSUE 5, DEC 2023

POLICY INSIGHTS

Cyber Security – pilot project for security cooperation between the EU and South Korea

Michael Reiterer
Ambassador of the European Union (ret.), Distinguished Professor, Centre for Security, Diplomacy & Strategy, The Brussels School of Governance

Keywords
cyber security, South Korea-EU cyber diplomacy, cyber defence, (cyber) deterrence, EU Cyber Diplomacy Toolbox

Article history
Submitted: 11 August 2023
Accepted: 15 November 2023
Published: 11 December 2023

Corresponding author
Michael Reiterer, Distinguished Prof.,
Centre for Security, Diplomacy and Strategy (CSDS)
Brussels School of Governance (BSoG)
Pleinlaan 2 Boulevard de la Plaine, B-1050
Brussels, Belgium
Email:michael.reiterer[at]vub.be

Introduction

The Republic of Korea, one of the five strategic partners of the EU in the Indo-Pacific, entertains not only a closely-knit framework of agreements with the EU but is also the only country which has concluded three comprehensive agreements (Framework Agreement/Free Trade Agreement/Crisis Management Framework Participation Agreement) with the EU.

Based on the Framework Agreement, a cyber dialogue is held with South Korea. This resulted in the conclusion of the Digital Partnership Agreement[1] in 2022 with the goal to foster joint work on semiconductors, next generation mobile networks, Quantum and High-Performance Computing, cyber security, artificial intelligence, platforms, data and skills.

South Korea excels technologically in IT-related matters and is one of the most connected societies worldwide. Therefore, cyber security became the pilot project of the 'Enhancing Security Cooperation in and with Asia' (ESIWA) program between the EU and Korea. The goal of the program is "to safeguard its citizens, defend the fundamental values upon which the Union is founded, including the protection of human rights, uphold the international rules-based system, promote multilateralism, contribute to regional stability, prevent violent conflicts and secure the Union's economic interests".[2] Cyber security, maritime security, counter-terrorism, CBRN-proliferation/disarmament and hybrid threats are ESIWA's key areas of engagement based on the recognition, that "European prosperity and Asian peace and security are closely connected", therefore, "the European Union has decided to strengthen its security cooperation in and with Asia."[3]

Cyber security, EU foreign policy and cyber diplomacy

Ever since the first Cyber Security Strategy of the EU was published in 2013, cyber security has become a top security priority. The security doctrine of the EU, the Strategic Compass, is clear on this issue: "We must also be able to swiftly and forcefully respond to cyberattacks, such as state-sponsored malicious cyber activities targeting critical infrastructure and ransomware attacks. To this end, we will reinforce our ability to identify and analyse cyberattacks in a coordinated manner. We will strengthen the EU Cyber Diplomacy Toolbox and make full use of all its instruments, including preventive measures and sanctions on external actors for malicious cyber activities against the Union and its Member States."[4]

Consequently, for geopolitical and geo-economic reasons, there is a need to integrate cyber security into the EU's foreign and security policy and to engage with third country partners – in particular in the Indo-Pacific region which houses many of the technological leaders. Cyber security has become a cross-cutting issue, concerned with an ever-increasing critical infrastructure e.g. structures essential to keep economies running, people connected or even alive.

Cyber diplomacy

Cyber diplomacy as part of the Common Foreign and Security Policy (CFSP) aims at conflict prevention, the mitigation of cyber security threats, and greater stability in international relations through rule setting, governance building but also in influencing potential aggressors. In protecting citizens and economies, cyber diplomacy includes deterrence which "complements or reinforces the established elements in the cyber diplomacy toolbox - capacity building, confidence-building measures, and cyber norms".[5] Countermeasures taken against malicious cyber activities under the EU Cyber Diplomacy Toolbox[6] need to be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity they respond to or aim to prevent.

In drawing on this Toolbox, the EU established in 2019 an autonomous sanction framework allowing "to impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member states, including cyber-attacks against third States or international organisations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP)".[7] Cyber-attacks falling within the scope of this sanction regime are those which have a *significant impact* and which originate or are carried out from outside the EU, or use infrastructure outside the EU, or are carried out by persons or entities established or operating outside the EU, or are carried out with the support of persons or entities operating outside the EU. Also only attempted cyber-attacks with a *potentially* significant effect are covered by this sanction regime. The EU used this tool for the first time in July 2020 and imposed a travel ban and an asset freeze on 8 individuals and 4 entities[8] (not states) in China, Russia and North Korea.

Criteria to define an attack or threat thereof, as well as how to deal with low-threshold attacks and their delimitation of legal intelligence or spying operations as well as of the scope of "critical infrastructure" would not only be legally desirable but also increase the deterrence value of countermeasures to be expected in return. The European Centre of Excellence for Countering Hybrid Threats, an autonomous, network-based international organization open to EU and NATO members, is tasked to support such endeavours – from soft power to military means, and from policy to practical questions.[9]

Determining the nature of the attack is important: neither need all attacks a response (proportionality test), nor does "every cyberattack need a cyber response. Criminal attacks should be handled as other crimes are handled – with vigorous prosecution."[10]

Linked to this issue is the question who oversees securing networks, a task which normally falls on the owner (private companies, state, or military). However, the omnipresence of digitalisation makes a growing number of networks part of 'critical infrastructure' whose securitisation and protection needs to be assured by public entities, either specialised agencies or the military.

1. European Commission (2022). European Union- Republic of Korea Digital Partnership. 28 November 2022; 10.1080/10357718.2021.1926423; at https://digital-strategy.ec.europa.eu/en/library/republic-korea-european-union-digital-partnership

2. EEAS (2018). Asia security cooperation: EU increases engagement on security in and with Asia. at https://www.eeas.europa.eu/node/45299_en (accessed 17 July 2023).

3. EEAS (2019). Factsheet Enhancing Security Cooperation in and with Asia. At https://www.eeas.europa.eu/sites/default/files/factsheet_eu_asia_security_july_2019.pdf

4. EEAS (2022) A Strategic Compass for Security and Defence. 21 March 2022; at https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

5. Mark Bryan Manantan (2021). Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. Australian Journal of International Affairs, 75:4; p. 441; at https://doi.org/10.1080/10357718.2021.1926423 This article includes a comprehensive overview of literature on cyber diplomacy in addition to an analysis of the bilateral relationship.

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

7. "Cyber-attacks: Council is now able to impose sanctions," Press Releases, EU Council, May 17, 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

8. "EU imposes the first ever sanctions against cyber-attacks," Press release, EU Council, July 30, 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

9. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE); at https://www.hybridcoe.fi/about-us/ (accessed 19 May 2023).

10. David Sanger (2018). The Perfect Weapon. Crown, New York, 2018; p. 303 (emphasis added).

The military domain and EU-NATO cooperation

In this respect, cyberspace has become the fifth domain of military operations, in addition to land, sea, air, and space and is therefore covered by defence policy. The 2014 EU Cyber Defence Policy Framework,[11] updated in 2018, defined six priority areas, including enhancing cyber defence capabilities of member states, protecting relevant communication channels, research and technology, training and deepening international cooperation, as there is "a need to ensure a dialogue with international partners, specifically NATO and other international organisations, in order to contribute to the development of effective cyber defence capabilities."[12]

To increase the force of deterrence, the Toolbox states that "malicious cyber activities" on one member state could result in a "joint EU diplomatic response", thus "reinforcing the security of the EU and its Member States".[13] This argument was taken up by NATO Secretary General Stoltenberg[14] – a major cyber-attack on a NATO member could trigger Article 5.

Thus, the EU and NATO recognise that similar threats are undermining "all levels of society in member states, threatening civil, political, economic and military security" and "the vast increase in the number of cyberattacks and the emergence of cyberspace as a new battlefield".[15]

In the 2023 Vilnius Summit Communiqué, NATO underlines, that its "deterrence and defence posture is based on an appropriate mix of nuclear, conventional and missile defence capabilities, complemented by space and cyber capabilities."[16] In relation to the four Indo-Pacific partners Korea, Japan, Australia and New Zealand, cyber defence, technology and hybrid are singled out as areas of cooperation "to tackle our shared security challenges … underpinned by our shared commitment to upholding international law and the rules-based international order".[17]

In short, cyber diplomacy aims at providing a "safe and secure cyberspace"[18] recognising that data has become the lifeline of the new and emerging technologies. A Cyber or Electronic Pearl Harbour –a scenario of a massive, unexpected cyber-attack on a country's critical infrastructure, which will immediately catapult two governments into a state of war"[19] – must be avoided.

The Indo-Pacific in the eye of the storm of attention

Recognising that their prosperity and security are interconnected, the ministers at the Second EU Indo-Pacific Ministerial Forum in Stockholm on 13 May 2023,[20] addressed and welcomed their growing engagement on a broad range of traditional and non-traditional security and defence-related issues, such as maritime security, cyber security, counterterrorism, crisis management, hybrid threats and transnational crime. European participants underlined that they had "stepped up security-related activities through the EU-funded project 'Enhancing Security Cooperation in and with Asia' (ESIWA),[21] which covers four thematic areas: counter-terrorism, cyber security, maritime security and crisis management. On Foreign Information Manipulation and Interference (FIMI), the EU is engaging with a number of partners as well as undertaking activities at regional level."[22] This builds on the first Ministerial Forum, held in February 2022 in Paris, fostering cooperation in the Indo-Pacific in applying the EU's Indo-Pacific Strategy[23] and the Global Gateway[24] Strategy. At this occasion the discussion on cyber security centred on the "importance of the UN normative framework for responsible state behaviour, the framework of international and regional instruments on organised crime and cybercrime including the Budapest Convention on Cybercrime as well as the strengthening of cyber resilience". The EU also seized this

11. Council of the European Union (2014). EU Cyber Defence Policy Framework. 18 November 2014; at https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf

12. Council of the European Union (2018). EU Cyber Defence Policy Framework (2018 update). 19 November 2018; at https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

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

14. BBC News, "NATO: Cyber-attack on one nation is attack on all," BBC News, August 27, 2019, https://www.bbc.com/news/technology-49488614.

15. Michael Reiterer (2022) "EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacific", in Boulet, Reiterer, Pacheco (eds.), Cybersecurity Policy in the EU and South Korea from Consultation to Action. Theoretical and Comparative Perspectives. Palgrave, 2022.

16. NATO (2023). Vilnius Summit Communiqué. 11 July 2023; at https://www.nato.int/cps/en/natohq/official_texts_217320.htm

17. Ibid., para 85.

18. Michael Reiterer (2022) "EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacific", in Boulet, Reiterer, Pacheco (eds.), Cybersecurity Policy in the EU and South Korea from Consultation to Action. Theoretical and Comparative Perspectives. Palgrave, 2022; p.18. This paper draws on the findings of this chapter.

19. Alan Collins (2022). Contemporary Security Studies. Oxford University Press, 2022; p. 429.

20. EEAS (2023). EU Indo-Pacific Ministerial Forum: Co-chairs' press release, 13 May 2023; at https://www.eeas.europa.eu/eeas/eu-indo-pacific-ministerial-forum-co-chairs%E2%80%99-press-release_en

21. EEAS (2019). Enhancing Security Cooperation in and with Asia. Factsheet; at https://www.eeas.europa.eu/sites/default/files/factsheet_eu_asia_security_july_2019.pdf

22. Ibid.

23. EEAS (2021). EU Strategy for Cooperation in the Indo-Pacific.16 September 2021; at https://www.eeas.europa.eu/sites/default/files/jointcommunication_2021_24_1_en.pdf

opportunity "to promote its 5G toolbox and the prospects for cooperation with the Indo-Pacific countries that it offers." [25]

Technology

The need to stay ahead in terms of technology to assure the security of production processes, supply chains and the resilience of societies became a recognised challenge. Thus, "a global race for leadership in key digital technologies or enabling systems…is increasingly characterised by international tension and a growing 'geopoliticisation' of digital technologies around the globe."[26] Otherwise the EU risks to become a rule-taker and no longer influence as rule maker. A lack of knowledge and loss of leadership in this area would present a danger to the security of critical infrastructure and essential services.

From the point of technology, European digital sovereignty is not achievable, and techno-nationalism will be counterproductive. The race for technological development and dominance is particularly strong in Asia, where Taiwan, South Korea and Japan are in the lead. While India and some ASEAN states are also entering the race, the rest of the world is concerned. Chris Miller, an economic historian, describes this ongoing race compellingly in his book ´Chip War´.[27] South Korea thus becomes a much sought-after partner due to its technological prowess. As technological progress constantly expands the frontiers of cyber, the mere concept of cyber diplomacy also expands in content and scope.

The EU's individualised cyber diplomacy – the case of South Korea

The Indo-Pacific is not only diverse politically, economically, culturally but also when it comes to mastering cyber technology. Therefore no one-size-fits all diplomacy can be applied: There are different groups of countries, ranging from those in the lead with some of them ahead of the EU and those catching up while others are clearly behind –in terms of technology but also defence e.g., vulnerability. South Korea is part of those leading in terms of technology.

The 2023 bilateral EU-South Korea Summit[28] confirmed the enhancing of security cooperation in general but also in the cyber field: resumption of the bilateral cyber policy consultation, meeting cyber threats, fighting cybercrime, fostering cyber governance in the UN to achieve results based on confidence building measures. False or misleading information is identified as threating democracy requiring joint efforts as part of a value based foreign policy. As a function of the later, "establishing relevant international rules on the use of Artificial Intelligence (AI) in the military domain" is identified as an area for cooperation and "the launch of the Responsible AI in the Military Domain Summit (REAIM), including the ROK's decision to host the 2nd Summit" is welcomed.

Areas to enhance EU-Korea cooperation – from consultation to action

As like-minded strategic partners sharing the same values, which the Yoon Administration underlines, there is potential for enhancing cooperation between the EU and South Korea as interests in politics, technological progress and in particular security meet. This is also corroborated by the recent volume on "Cyber security Policy in the EU and South Korea from Consultation to Action" edited by Gertjan Boulet, Michael Reiterer and Ramon Pacheco Pardo.[29] The following identification of possible areas of cooperation between the EU and the Republic of Korea draws on the findings of the Korean, European and US and Chinese authors of this edited volume.

Reflecting the shared values approach, human-centric digitalisation, master-

24. European Commission/High Representative (2021). The Global Gateway. 1 December 2021; at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021JC0030 See also European Commission (2021). 2030 Digital Compass: the European way for the Digital Decade. 9 March 2021; at https://commission.europa.eu/system/files/2023-01/cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf

25. EEAS (2022). Ministerial Forum for Cooperation in the Indo-Pacific. 22 February 2022; at https://www.eeas.europa.eu/eeas/ministerial-forum-cooperation-indo-pacific_en

26. European Political Strategy Centre (European Commission), Rethinking Strategic Autonomy in the Digital Age (EPSC Strategic Notes no. 30, July 2019), 2, https://op.europa.eu/en/publication-detail/-/publication/889dd7b7-0cde-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-118064052.

27. Chris Miller (2022). Chip War. The Fight for the World's Most Critical Technology. Simon&Schuster, 2022.

28. European Council (2023). Joint statement European Union - Republic of Korea Summit 2023. Seoul, 22 May 2023; at https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2863

29. Gertjan Boulet, Michael Reiterer, Ramon Pacheco Pardo (eds.). Cybersecurity Policy in the EU and South Korea from Consultation to Action. Theoretical and Comparative Perspectives. Palgrave, 2022; p. 292.

ing the ethical challenges of the emerging technologies and the ethical implementation of AI technologies are a common overarching goal which can be developed and adapted in the high-level dialogue on the digital economy. The adequacy of the protection of private data between the EU and the Korean governments based on the General Data Protection Regime (GDPR) is a trust building measure and serves as a basis for further collaborative steps.

Emerging technologies pose challenges in the technical cooperation, including the organisation of joint research and the issue of solving intellectual property issues. Given the importance of norms and standard setting for international competition as well as resilience of economies, the development of compatible certification schemes is not a technical but highly political issue. Because of the link to resilience, joint exercises and scenario planning are necessary beyond information sharing. This should lead to an increase of joint research projects meeting the concerns of both partners. It also includes the need to ensure that their various agencies involved in cyber security cooperate.

Concerning norm-building in the cyber domain it is necessary to draw on the experience of the private sector. Stringent norms for hardware standards would also enhance the security of networks as the 5G discussion has shown; as work for 6G is already underway, this aspect is of particular importance and interest to the EU and Korea for geopolitical but also commercial reasons, as the US pursues a restrictive policy where partners and allies should have their own solutions.

Cyberspace is borderless. Therefore, conflict prevention can be compared to a chain, the weakest point determines the strength of the chain. The EU and South Korea share this view and have identified capacity building leading to confidence building as an important tool for cyber conflict prevention. They have both identified regional organisations such as the OSCE and ASEAN as partners for capacity building, in areas where they respectively have special experience.

Cyber security is also a function of cyber defence where deterrence is important. Attributing a cyber-attack is a technically difficult task but necessary for implementing countermeasures, be it legally, through sanctions or in military terms by means of counterstrike. Joining of information and technological know-how would be a mutual asset.

The first step is to determine whether a cyber-attack has taken place, as not all intrusions in the cyber realm are automatically illegal, with borderlines to draw between espionage, information collection and cyber-attacks. According to international law, countermeasures have to be proportional and need to be taken in the same area, e.g. cyber.

A combination of intelligence gathering and intelligence-sharing with like-minded partners, joint work to anticipate and mitigate the effects of cyber-attacks, and measures to ensure that the population is resilient against psychological cyber warfare (e.g. misinformation campaigns) are all necessary.[30] South Korea could share its experience with intelligence gathering and sharing, if not with the EU, then at least with some member states. And in fact, the launch of the Five Eyes (United States, the United Kingdom, Canada, Australia, New Zealand), and the Five Eyes Plus (France, Japan, South Korea) framework in late 2019 focusing on the North Korean threat scenario is an opener for the cooperation with the EU as France is a Plus-member.

To allow for transparency, which contributes to deterrence, the EU launched a legislative act to impose cyber sanctions on third parties in May 2019.[31] Only a year later, in July 2020 the EU imposed its first-ever cyber sanctions, targeting individuals and entities –not states – in China, North Korea, and Russia.[32] One

30. Maximilian Ernst and Sangho Lee, 'Countering Cyber Asymmetry on the Korean Peninsula: South Korea's Defense against Cyber Attacks from Authoritarian Sates', *Journal for Intelligence, Propaganda and Security Studies,* Vol. 15, No. 1 (2021): pp. 165-179.

31. Council of the European Union, *Council Decision Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union and its Member States,* 14 May 2019, available at https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf (accessed 26 November 2021).

32. Council of the European Union, *EU Imposes the First-Ever Sanctions Against Cyber-Attacks,* 30 July 2020, available at https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/ (accessed 26 November 2020).

of the authors of the volume, Joohee Park, comes to the conclusion that South Korea, which does not have such a framework, could be interested to join the EU and other actors such as the US by imposing cyber sanctions jointly. Thus, a multilateral framework would increase effectiveness and open the door to defensive actions for those who are hesitant for geopolitical reasons to act alone. The EU could not only share experience with South Korea but entice Korea to join such a framework. As a first step, in February 2023 the Korean government put sanctions on North Korean entities "linked organizations for their alleged involvement in illegal cyber activities as a means to fund the country's nuclear weapon and missile program. The movement is largely symbolic, as it is the first ever unilateral sanctions against North Korea's cyber threats."[33]

There is also a strong values-based element to it: in the context of the divide between democracies and autocracies, democracies have woken up to the need to assure the security of those parts of their critical infrastructure, which assure the core functions of democracies, such as elections. Securing democratic processes is in turn linked to fighting fake news and propaganda, as citizens need real and objective information to base their political decisions on. This requires protection against cyberattacks in enforcing standards and regulations to ensure that harmful programmes do not have the desired effects, restricting malicious behaviour, and making use of sanctions. Developing pan-EU cyber defence capabilities thus entails the need for the EU to advance cutting-edge technologies to command the operational capability necessary to prevent, deter, and respond to cyber-attacks.

In cooperating to develop the above-mentioned Responsible AI in the Military Domain Summit (REAIM), the EU and South Korea could take joint initiatives. However, an international agreement on the use of AI will take considerable time to develop, especially with regards to the difficult situation the UN faces in establishing the markers of responsible state behaviour, even further complicated by the war in Ukraine. The goals to safeguard AI infrastructure could be to assure human oversight for AI use particularly in the military field (autonomous weapons systems) and to set standards as a catalyst for the international community to follow the example.

In this context, the authors of the volume draw attention to the difficulty of democracies in general to implement highly effective defence mechanisms against cyber-attacks because of restraints posed by fundamental rights. Nevertheless, the rights of citizens must be protected and therefore deterrence and response capabilities to protect these rights have to be enhanced. To achieve this goal the centralization of cyber defence command capabilities has turned out to be useful, but has to be discussed and evaluated in the respective political and legal environment. Furthermore, this not only an organisational matter, but has a strong human rights element because of the need to exercise democratic control over powerful cyber authorities, an area where South Korea and the EU can learn from each other.

Developing rules and regulations to foster not only the rule of law but also to guarantee a free and open internet is another common, values-inspired goal. While the UN should be at the centre of this endeavour, the organisation is unlikely to find common ground in the foreseeable future because of the split into two "camps" which approach the problem from very different angles: either applying existing international law or concluding a new treaty. This reflects a deep seated and rather ideological split on the understanding of whether keeping cyberspace secure and safe means keeping it secure for transactions or safe content-wise. The same applies to the notion of ´openness´: it is not clear whether it refers to functionality or ideology.

33. Kuksung Nam and Dain Oh (2023). The Readable Feb. 10, 2023 updated Feb. 14, 2023; at https://thereadable.co/weekend-briefing-south-korea-issued-sanctions-on-north-korean-hackers/

Thus, the EU and South Korea could take the lead in advancing cyber governance, to create momentum for a broader based regulation, where again the OSCE and ARF could play an important role as regional steppingstones to achieve a global solution. Clear international norms reduce ambiguity around the applicability of international law and norms. As one of the authors, Mason Richey, put it succinctly, a "lack of norms [...] incentivizes predatory behavior"[34] leading to a sort of cancer undermining cyber security to a degree that the elimination of cyber threats or attacks is realistically no longer possible. Therefore, it remains to "mitigate cyber escalation risk".[35]

Concerning cybercrime, the EU and South Korea have different legislative frameworks. However, they can engage in information sharing, consultations to make legislation compatible with the Budapest Convention (established by the Council of Europe and entered into force in 2004), exchanging best practices, and developing multi-stakeholder initiatives. The widely differing views on the Convention and its further development are also reflected by the authors of this volume. This can be exemplified by the treatment of digital evidence regulated in the Second Additional Protocol to the Budapest Convention (as approved by the Committee of Ministers on 17 November 202)[36]. The approach chosen has a direct bearing on e-justice and the mode of cooperation among parties. In the volume opposing views held by Tatiana Tropina and Gibum Kim on handling e-evidence illustrate the issue. The human-centred approach of the EU and South Korea makes them pristine candidates to play a leading role in these endeavours. As data is the lifeline of the nascent economy, leadership in this highly complex and competitive area of cyber will also grant economic and societal advantages.

The EU-Korea High Level Conference on Cyber security (30 June 2023),[37] following the first meeting of the Digital Partnership which had identified joint cyber security research, cyber threat information sharing and policy exchanges, offered a stock-taking opportunity in partnership with industry and academia. There is a common need to move beyond 'traditional' malware criminality to ward off hybrid attacks as part of geopolitical competition and conflicts. Cooperation of the respective Information Sharing and Analysis Centres (ISACs) is important to improve cyber security as well as mutual capacity building. These efforts have its anchor in the Digital Agreement but need vigorous implementation beyond words but through deeds.

Conclusions

EU cyber diplomacy is guided by a few principles, which like-minded countries like South Korea share. Firstly, protecting critical infrastructure is in the interest of the functioning of societies and economies. The positive element is that this is a permanently growing denominator, as cyberspace is permanently expanding because of technological progress.

Secondly, the role of the private sector gains greater relevance. The giant tech companies, whether in the production of hardware (high-end semiconductors, 5G and 6G technologies, quantum computing) or of software like the Alphabet companies and the developers of Artificial Intelligence (AI), are in the driving seat of development and research. Public actors must cooperate with them, whether in form of public private partnerships supporting technological development or in regulating their behaviour.

The latter aspect also plays an important role in the application of AI to the military sector: autonomous weapons systems are those that select and apply force to targets without human intervention.[38] The United Nations is active in

34. Mason Richey (2022).Cyber Offence Dominance, Regional Dynamics, and Middle Power–led International Cooperation. In Boulet, Reiterer, Pacheco (eds.), Cybersecurity Policy in the EU and South Korea from Consultation to Action. Theoretical and Comparative Perspectives. Palgrave, 2022; p.69.

35. Mason Richey (2022), p.87.

36. Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence.* 7 November 2021, at https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

37. Cyber Security That Matters (2023). Full scripts at https://thereadable.co/full-scripts-eu-rok-high-level-conference-on-cybersecurity-june-30-2023/

38. International Committee of the Red Cross (ICRC). What you need to know about autonomous weapons. At https://www.icrc.org/en/document/what-you-need-know-about-autonomous-weapons#:~:text=Autonomous%20weapon%20systems%2C%20as%20the,when%20that%20strike%20will%20occur (accessed 16 May 2023).

this field of lethal autonomous weapons systems (LAWS) which lead in 2019 to the adoption of 11 Guiding Principles.[39]

Michael Zinkanell, contributor to the edited volume, opens in this context another venue for cyber diplomacy, namely the necessity to regulate the use of AI in autonomous weapons systems. "In order to prevent the risks and threats of AI, it is necessary to scrutinise the intersection of AI, cyber security and cyber arms control mechanisms."[40] Working with countries to get them on board is at the crossroad of disarmament and cyber diplomacy.

Concerning arms control, Kissinger/Schmidt/Huttenlocher describe the task of future cyber arms-control negotiators "to solve the paradox that discussion of a cyber weapon's capability may be one and the same with its forfeiture (permitting the adversary to patch a vulnerability) or its proliferation (permitting the adversary to copy the code or method of intrusion)."[41]

Thirdly, and with some similarity to LAWS, the prevention of cyber criminality is another common denominator. This is a feature in the interest of technological haves or have-nots, as they are not spared malware for ransom from enterprises, state actors or private persons, or child pornography, sexual harassment or hate speech. Strengthening e-justice through judicial cooperation adapted to the new cyber environment and the promotion to the accession to the only international agreement for fighting cyber criminality, the Budapest Convention and its Protocols, are challenges for cyber diplomacy. This also includes the fourth common denominator, the interest to fight fake news and propaganda as well as interference into domestic processes.

As Commissioner Thierry Breton put in in Seoul, "Cyber security has become a global emergency."[42] Thus, cyber security and consequently cyber diplomacy are a cross-cutting topic, where technological knowledge plays and an important role; it also reaches deep into defence. As cyber space is borderless, it is an obvious case where only joint action can produce security. Nevertheless, the looming danger of an ideologically split internet is real and could further enhance the balkanisation of the internet, leading to more fragmentation, conflict and ´unpeace´ instead of connectivity, as Mark Leonard put it.[43]

Cyber security is not only a technical or technological issue but has developed into a core political issue with strong defence implications. Increasing resilience such capacity building to withstand attacks on various levels is the EU's approach as it also leads in turn to deterrence. Because of the cross-cutting nature cyberspace and the omnipresence of semiconductors, cyber resilience increases at the same time resilience against conventional risks linked to critical infrastructure.

Resilience should bend the overall cost-benefit calculation in favour of the defender. As Joseph S. Nye[44] points out, this also depends on the relationship of the attacker with the target creating links to potential adversaries so that any attack they launch will likely harm their own interests, too. What he calls '*entanglement,*' e.g. interdependence, is a stabilising factor as opposed to asymmetric relationships.

Like any security policy cyber security and its implementation through cyber diplomacy is not cost-free and needs long-term political and financial cross-cutting commitments to allow coherent policy planning and implementation to assure the ultimate goal, and stability in the all-important cyber space.

Cyber diplomacy helps winning the battle for digital governance as, "whoever wins the global debate over the rules, standards, and norms that govern data privacy and data flows, technology standards, cyber security, and critical technologies will have a major competitive advantage in the economy of 2030".[45]

39. United Nations. Background on LAWS in the CCWM; at https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/ (accessed 17 May 2023).

40. Michael Zinkanell (2022). Arms Control in the Cyber Domain: A European Approach to Mitigate Digital Threats. In Boulet, Reiterer, Pacheco (eds.), Cybersecurity Policy in the EU and South Korea from Consultation to Action. Theoretical and Comparative Perspectives. Palgrave, 2022; p.150.

41. Henry A. Kissinger, Eric Schmidt, Daniel Huttenlocher (2021). The Age of AI. Little, Brown and Company, New York; pp. 152-153.

42. Keynote speech at the EU-ROK High Level Conference on Cybersecurity, June 30, 2023. Cyber Security That Matters.

43. Mark Leonard (2021). The Age of Unpeace. Bantam Press, 2021; p. 114.

44. Joseph S. Nye (2022). The End of Cyber-Anarchy? How to Build a New Digital Order. Foreign Affairs, January/February 2022.

45. Matthew P. Goodman, "Time to Align on Digital Governance," Commentary, Center for Strategic & International Studies, January 24, 2020, https://www.csis.org/analysis/time-align-digital-governance.

The EU and South Korea share the will and determination to be on the side of the winners, they have the capacity and must bundle activities to reach this goal in moving from consultation to action.