Trends of Digital Transformation Based on the UN, EU, and NATO Experiences

Khatuna Burkadze

INTRODUCTION

Digital technologies have profoundly affected various aspects of people's lives from the economy to healthcare. Governments have struggled to implement norms that enable digital innovation while protecting consumers, users, and democratic institutions.[1] In 2016, World Economic Forum Founder and Executive Chairman Klaus Schwab used the title of his book, *The Fourth Industrial Revolution*, as the umbrella term describing the process of how technology has come to impact all aspects of society. Artificial intelligence (AI), fifth-generation mobile networks (5G), three-dimensional (3D) printing, cloud computing, robotics, unmanned aerial vehicles (UAVs), augmented reality, the Internet of Things (IoT), genomics, biometrics, and blockchain are commonly included in the list of present-day emerging technologies anticipated to assist human societies to overcome

Dr. Khatuna Burkadze, *graduate of The Fletcher School, has been a Fulbright scholar at the MIT Center for International Studies as well as a visiting professor at Columbia University, Bard College, and The Fletcher School. She has successfully completed programs on negotiations and security studies at Harvard University and the George C. Marshall European Center for Security Studies. Dr. Burkadze is an alumna of the U.S. Department of State's Program on American Foreign Policy as well as the author of dozens of articles and book chapters. Dr. Khatuna Burkadze has working experience in legislative, executive and judicial governmental branches. Particularly, she has been employed by the Parliament, Ministry of Foreign Affairs, Office of the Prime Minister and Supreme Court of Georgia. Currently, Professor Burkadze delivers lectures at Business and Technology University in Tbilisi, Georgia.*

global challenges.[2] The speed, scope, and scale of digital advances and diffusion in this revolution are unlike anything the world has ever seen before.[3]

The UN's 2030 Agenda for Sustainable Development aims to build dynamic, sustainable, innovative, and people-centered economies in a transforming world. To this end, governments, international organizations, the business sector, and other non-state actors and individuals should contribute to strengthening developing countries' scientific, technological, and innovative capacities to move toward more sustainable patterns of consumption and production.[4] Adopting an innovative and technological agenda is a good way to create new opportunities and find solutions in this changing environment, as well as to take action in line with the international sustainable development goals. Adopting such an agenda can also play a significant role in achieving higher levels of economic productivity.

The expansion of the internet has allowed billions of people access to information and has connected individuals in ways that were not previously possible.[5] As for AI, it is a tool that automates routine technological tasks in different fields (healthcare, education, the justice system, foreign and security policies, etc.) through the use of robots as re-programmable multi-purpose devices.[6] AI is evolving fast. The importance of digital advances has increased during the pandemic; they have become significant instruments in the continual performance of remote tasks.

Given that digitalization is advancing at an unprecedented pace, it is imperative that global and national decision makers understand what is driving digital development and where trends in digitalization will lead the global world.[7] These decision makers must develop clear approaches to governing the digital space.[8] This is especially important since digital transformation is supported by affordable communications and cheap devices that can introduce new risks.[9]

Overall, the digital revolution facilitates cooperation on digital issues in international organizations. International actors are developing digital policies and institutional instruments to achieve their own goals and mitigate technological risks in the 21st century. In this regard, the article examines core elements of digital transformation based on the experiences of global (e.g., the UN) and regional (e.g., EU and NATO) actors. An analysis of digital trends is significant because it illustrates how technological advances shape the structures of both global and regional international organizations. It would promote the development of the international digital agenda with the focus on elaborating new visions for the effective use of technological advances in various fields and overcoming digital challenges in the future.

DIGITAL COOPERATION AND TRANSFORMATION: THE VISION OF THE UNITED NATIONS

The Secretary-General of the United Nations, *António Guterres, stated, "A safe, inclusive, and equitable digital future is essential for progress and peace."*[10] In 2020, Guterres launched the Roadmap for Digital Cooperation, offering a vision for international digitalization of the world. According to Guterres, the digital world is based on the following key principles: "Connect, Respect and Protect." These principles indicate that digital tools should serve as means for development rather than a source of harm or inequality.[11]

Building upon the Roadmap, the High-level Panel on Digital Cooperation developed in 2020 made the following five recommendations: (a) build an inclusive digital economy and society; (b) develop human and institutional capacity; (c) protect human rights and human agency; (d) promote digital trust, security, and stability; and (e) foster global digital cooperation. These recommendations aim to enhance international digital cooperation to optimize the use of digital technologies and mitigate their risks.[12]

A central challenge to building an inclusive digital economy is that there are no baselines concerning the level of digital connectivity required to access the online space. Identifying such baselines, with the flexibility to update them as necessary in light of technological changes, would enable the development of equitable targets. Risk factors that affect the ability of vulnerable groups to access connectivity should be specifically identified and addressed.[13]

Indeed, international organizations are currently seeking to address this very issue. As part of the multi-stakeholder consultation process, coordinated by the International Telecommunication Union (ITU) and UNICEF and supported by the Office of the Envoy on Technology, ITU's Data and Analytics Division is leading a multi-stakeholder working group to develop a baseline framework for universal and affordable digital connectivity.[14]

The UNICEF-ITU initiative to connect all schools around the world to the internet is a good example of accelerating connectivity. As of March 2021, it has mapped over 800,000 schools globally, and 19 countries have formally joined the initiative. Almost 3,000 schools have been connected as part of pilot projects in Kenya, Sierra Leone, Kazakhstan, Brazil, and the Organization of Eastern Caribbean States.[15] Named "Connecting Every School to the Internet – GIGA," the global initiative aims to connect every young person to information opportunity and choice. It seeks to develop and launch a global financing instrument for school connectivity, as well as

country-level capital market products that examine and prototype innovative financing modalities. GIGA's initiative directly responds to ITU's call for affordable connectivity financing. With an estimated price tag of $428 billion, ITU hopes to connect the remaining three billion people aged ten years and above to broadband internet by 2030.[16]

Globally, efforts must be better coordinated and scaled up. A set of metrics to measure digital inclusion will be essential for evidence-based policymaking. Everyone should have an equal opportunity to be empowered by information and communication technologies. Empowerment means accessibility through not only physical access and skills development, but also through inclusive designs that respect the needs of all people, including people with disabilities, language barriers, structural barriers, and intersectional identities—while taking into account the importance of locally relevant content.[17]

Furthermore, the need for digital capacity-building is crucial. Achieving sustained progress in the dimensions of digitalization requires skills development especially in developing countries. This is necessary in order to ensure that emerging technologies are used most effectively and that individuals remain protected and productive online.[18] In the context of human rights, digital technologies provide new tools that may be used to advocate, defend, and exercise fundamental rights, but they may also be used to violate them. Furthermore, existing human rights treaties were signed in a pre-digital era. In the current world, where online violations can lead to offline abuses, the internet cannot be an ungovernable space. Human rights exist online as they do offline and have to be respected and safeguarded in full.[19]

Digital stability requires developing standards and institutional instruments to avoid threats. In the cyber era, information technologies may have a disruptive effect as computers can be used to launch new forms of attacks. In order to combat cyberattacks at the global level, the International Telecommunications Union (ITU), as a constituent part of the UN, adopted international regulations governing the electromagnetic frequency spectrum. The organization's agenda also includes the development of a global information infrastructure. In developing standards for online security and digital certificates, the ITU could attempt to elaborate standards for dealing with new forms of information warfare.[20] Because of the significance of satellites for international telecommunications, as well as for military command, control, and intelligence, some forms of cyber warfare may involve orbital assets and may therefore implicate the ITU and other telecommunication regulators.[21]

The United Nations established a Group of Governmental Experts (UN GGEs) in 2004 to strengthen the security of global information and telecommunications systems. The UN GGEs has been lauded for mapping the current state of play in international cyber affairs and promoting the view that cyberspace is not a digital "Wild West" where no rules apply.[22] Particularly, the UN GGEs has highlighted that the UN Charter applies to the digital space. States agree that they have jurisdiction over the information and communication technology (ICT) in their own territories, and that states should not perpetrate internationally wrongful acts either themselves or through proxies.[23]

The UN GGEs further underscores that norms do not seek to limit or prohibit action that is otherwise consistent with international law. Instead, norms reflect the expectations of the international community and set standards for responsible State behavior. Norms help to prevent conflict in the ICT environment and contribute to its peaceful use, which in turn enables social and economic development.[24]

> In 2018, another UN-mandated working group—the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG)—was established in parallel with the UN GGEs.[25] OEWG confirms that international law, and in particular the Charter of the UN, is applicable to cyberspace. Norms do not replace or alter states' obligations or rights under international law—which are binding—but rather provide additional and specific guidance on what constitutes responsible state behavior in the use of ICTs.[26] The report recommends that states voluntarily identify and consider confidence-building measures (CBMs) appropriate to their specific contexts and cooperate with other states on their implementation. The report also outlines comprehensive capacity-building measures in the field of ICT security.[27]

As for global digital cooperation, the existing digital cooperation architecture has become highly complex and diffused. Moreover, global discussions and processes are often not inclusive enough. This situation is exacerbated by the lack of a common entry point into the global digital architecture, which makes it especially hard for developing countries, small- and medium-sized enterprises, marginalized groups, and other stakeholders with limited budgets and expertise to make their voices heard. Member states are considering working with a multi-stakeholder task force to pilot the distributed co-governance model at the national or regional levels.[28]

Equitable access to digital emerging technologies, such as AI and quantum computing, will allow the international community to reap the benefits of digitalization and adapt to the future of work.[29] Artificial intelli-

gence is ubiquitous in its applications, ranging from navigation and content recommendations to explorations of genome sequencing. Its use was forecasted to generate nearly USD 4 trillion in added value for global markets by 2022 before the COVID-19 pandemic, [30] which experts predicted may change consumer preferences and open new opportunities for AI-led automation in various fields.[31]

In light of the above, the UN developed a set of recommendations for building digital economies and societies, enhancing digital capacities, protecting human rights in the digital world, promoting digital trust, security, and stability, and fostering global digital cooperation. However, greater digital cooperation requires reaching consensus among UN member states, especially around defining digital norms. The establishment of the OEWG in parallel with the UN GGEs has illustrated that member states of the UN have a lack of common understanding of norms for operating in the digital world. Clearly, there are some ambiguities on the applicability of international humanitarian law in cyberspace. Given rapid technological changes during the pandemic, it is important to develop and implement new international projects that provide equal access to digital advances around the world and enhance instruments that protect the right to privacy and mitigate digital risks.

SHAPING EUROPE'S DIGITAL FUTURE: THE VISION OF THE EUROPEAN UNION

When European Commission President Ursula von der Leyen assumed office, enhancing digital capabilities across the European Union immediately emerged as a top priority. Specifically, Von der Leyen called for Europe to achieve "technological sovereignty in some critical technology areas."[32] The COVID-19 pandemic further reinforced the significance of digital policymaking for both national governments and European institutions, as individuals found themselves working remotely on platforms with questionable security.[33]

In March 2021, the European Union (EU) adopted the 2030 Digital Compass, which set the EU's digital ambitions for 2030. The Compass established a monitoring system and outlined key milestones and the means for achieving these ambitions. According to the Digital Compass, Europe will be digitally sovereign in an interconnected world by building and deploying technological capabilities to empower people and businesses to seize the potential of the digital transformation and enable them to build a healthier and greener society.[34]

The European way to a digitalized economy and society is about solidarity, prosperity, and sustainability, and is anchored in the empowerment of its citizens and businesses. By adhering to these principles, the EU aims to ensure the security and resilience of its digital ecosystem and supply chains. The Compass seeks to track the EU's pace of digital transformation, gaps in its strategic digital capacities, and the implementation of European digital standards.[35]

The 2030 Compass highlights that Europe will only achieve digital leadership by building a sustainable digital infrastructure regarding connectivity, microelectronics, and the ability to process vast data in conjunction with other technological developments and support for the industry's "competitive edge". In terms of enhancing international cooperation, the EU has proposed to establish a new EU-U.S. Trade and Technology Council to deepen trade and investment partnerships with the United States, strengthen joint technological and industrial leadership, develop compatible standards, deepen research collaboration, promote fair competition, and ensure the security of critical supply chains.[36] The EU will work actively to promote its human-centered vision of digitalization within international organizations, in cooperation with member states and like-minded partners. This coordinated approach should especially defend the use of technology that is fully adherent to the UN Charter and the Universal Declaration on Human Rights.[37]

The EU has a clear vision of the development of AI. Through the Digital Europe and Horizon Europe programs, the Commission plans to invest EUR 1 billion per year in AI and mobilize additional investments from the private sector and the member states to reach EUR 20 billion investment per year over the course of this decade.[38]

AI and other digital technologies can contribute to a sustained post-COVID-19 recovery due to their potential for increasing productivity across all economic sectors, creating new markets, and bringing tremendous opportunities for Europe's economic growth.[39] Also, AI can be a strategic tool to counter current challenges, including hybrid threats. AI can help to fight crime and terrorism by enabling law enforcement to keep pace with the fast-developing technologies used by criminals in support of their cross-border activities. At the same time, the use of AI also creates risks that need to be addressed. Certain characteristics of AI, such as the opacity of its algorithms, pose potential high risks to public safety and the fundamental rights of individuals. Unfortunately, existing legislation is unable to address these issues.[40]

In its Communications of April 25 and December 7, 2018, the

European Commission set out its vision for AI, which supports "ethical, secure and cutting-edge AI made in Europe."[41] The aim of the Guidelines is to promote trustworthy AI. Trustworthy AI has three components, which should be met throughout the system's entire life cycle: (1) it should be lawful, complying with all applicable laws and regulations; (2) it should be ethical, ensuring adherence to ethical principles and values; and (3) it should be robust, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm. Each component in itself is necessary but not sufficient for the achievement of trustworthy AI. Ideally, all three components will work in harmony and overlap in their operation. If, in practice, tensions arise between these components, society should endeavor to align them.[42]

On April 21, 2021, the European Commission proposed a new legal framework to govern the use of AI within the EU. The proposal develops a risk-based approach whereby the uses of AI are categorized and restricted according to whether they pose an unacceptable, high, or low risk to human safety and fundamental rights. The policy is widely considered to be one of the first of its kind in the world and would have profound and far-reaching consequences for organizations that develop or use AI.[43]

The aforementioned EU AI Act aims to address the risks stemming from the various uses of AI systems and promote innovative approaches in the field of AI.[44] Mark MacCarthy, a nonresident senior fellow at the Brookings Institution, and Kenneth Propp, a senior fellow at the Europe Center of the Atlantic Council, have called the proposed regulation "a comprehensive and thoughtful start to the legislative process in Europe that might prove to be the basis for trans-Atlantic cooperation."[45]

In an effort to safeguard data privacy, the EU drafted and passed the General Data Protection Regulation (GDPR) that was put into effect on May 25, 2018. It imposes obligations onto organizations anywhere in the world, so long as they target or collect data related to people in the EU.[46] With the GDPR, Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data to cloud services and breaches are a daily occurrence. The regulation itself is large and far-reaching, but fairly light on specifics, making GDPR compliance a daunting prospect, particularly for small- and medium-sized enterprises (SMEs).[47]

To achieve a high common level of cybersecurity across Europe, the EU established the European Union Agency for Cybersecurity (ENISA) in 2004. ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products and services, and cooperates with member states and EU

institutions to overcome cyber challenges. Through knowledge-sharing, capacity-building, and awareness-raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, boost the resilience of the Union's infrastructure, and keep European citizens digitally secure.[48] However, the COVID-19 pandemic has highlighted the need for more security in the digital world. As people increase their presence online to maintain personal and professional relations, cybercriminals target e-commerce and e-payment businesses, as well as the healthcare system. The ENISA focuses on working towards a trusted and cyber-secure Europe in cooperation with the wider international community.[49]

Overall, the EU assists its member states in developing standards and establishing institutional mechanisms for the effective implementation of digital policies. The ethical and legal frameworks of the EU create guarantees that safeguard fundamental rights, such as the right to privacy, and prohibit the use of machines that can cause damages in various aspects. The EU's risk-based approach promotes the use of secure applications and the protection of basic rules. Also, the EU is actively proposing initiatives to enhance international digital cooperation with its partners.

NATO'S DIGITAL TRANSFORMATION

The COVID-19 crisis has demonstrated, in a dramatic and unexpected fashion, the deleterious effects that pandemics can have not only on the public health of NATO citizenries, but also on their social resilience and security, both by reorienting policy attention and scarce resources and fueling international rivalry and confrontation. Indeed, the COVID-19 pandemic has accelerated the digitalization of NATO societies.[50] The digital era, with its rapid technological change and global interconnectivity, has boosted the appeal and power of these methods, amplifying their speed, scale, and intensity. Hybrid attacks and cyberattacks are threats to societies, employed as tools by hostile actors, states, and non-state actors alike. It is difficult to detect the origins of such attacks, as states sometimes use proxies. These attacks undermine international order and democratic systems.[51]

NATO formulated its mission in cyberspace—to protect its own networks, enhance the capabilities of the member states, and to cooperate with partners after suffering its first major cyberattacks in 1999—during Operation Allied Force. This mission was established in response to incidents that included denial-of-service attacks and defacements of the webpage for the Supreme Headquarters Allied Powers Europe, as well as defacements to the online infrastructure of the U.S. military.[52]

Former Secretary of Defense of the United States Ash Carter said, "The 20th century NATO playbook was successful in working toward a Europe whole, free, and at peace, but the same playbook would not be well-matched to the needs of the 21st century. Together with our NATO allies, we must write a new playbook, which includes preparing to counter new challenges like cyber and hybrid warfare."[53]

This playbook will provide a new smart strategic vision for a smarter NATO. It will clarify key characteristics of cyber and hybrid behavior and develop appropriate means to overcome modern challenges. The common understanding facilitated by this playbook of new forms of warfare and their possible destructive nature can mitigate cyber risks.

To examine the public international law governing cyber warfare, the NATO Cooperative Cyber Defense Center of Excellence launched a major research project in late 2009.[54] In Tallinn Manual 1.0 and Tallinn Manual 2.0, international experts analyze how existing international law applies to cyber warfare and cyber operations.

At the Wales Summit, member states of NATO decided that, "Our policy recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyberattacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. A decision as to when a cyberattack would lead to the invocation of Article 5 of the North Atlantic Treaty would be taken by the North Atlantic Council on a case-by-case basis."[55] This means that member states of the Alliance agreed that international law applies to cyberspace, but whether or not to invoke Article 5 is a decision that will be made by NATO based on the particular case. Therefore, the principle of collective defense is not automatic, but mostly dependent on legal analysis of the scope, scale, and speed of destructive action carried out by the international actor. If a cyberattack causes substantial damage and reaches a threshold that threatens peace and security, it rises to the level of armed attack. In such cases, Article 5 could be invoked by the Allies.

Furthermore, at the Warsaw Summit in July 2016, the Allies recognized "cyberspace as a domain of operations, in which, NATO must defend itself as effectively as it does in the air, on land, and at sea."[56] On February 10, 2016, NATO and the EU concluded a Technical Arrangement on Cyber Defense to help both organizations better prevent and respond to cyberattacks. This Technical Arrangement between NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the EU (CERT-EU) provided a framework for exchanging information and sharing best practices between emergency response teams.[57] In

2018, the Alliance created Counter Hybrid Support Teams (CHSTs) to provide tailored assistance to the member states. In 2019, NATO approved the Report on Enhancing NATO's Response to Hybrid Threats, which outlined priorities and an agenda for countering hybrid threats. Despite these advances, NATO must remain vigilant about its cyber hygiene.[58]

NATO's digital agenda mostly contains issues related to the challenges of ICTs. By creating such an agenda, NATO has strengthened its existing instruments and created a new structural mechanism for the protection of communication networks. The North Atlantic Alliance assists its member states and partner countries to enhance their cyber capabilities. Also, the Allies decided that cyberattacks can trigger Article 5 of the North Atlantic Treaty and cyberspace represents a domain of operations. The North Atlantic Treaty applies to cyberattacks because they can reach a threshold that threatens national and regional security, and because their impact can be as harmful to societies as conventional attacks. This approach allows member states of the Alliance to define rules in the digital space and mitigate risks more effectively.

CONCLUSION

At the global level, rapid technological advances and ambiguities of international norms require the development of new approaches and views for clarifying notions of digital behavior. The digital world does not have boundaries, and there is no global consensus and understanding on legal aspects of digital space. In this regard, Russia, China, and many like-minded countries have different concepts of the applicability of international law to the digital world. These states could potentially operate in the digital space according to different understandings of what is permissible under international norms, including international humanitarian law.[59] A reinterpretation of the international legal framework means providing new explanations of existing norms. As mentioned by Professor Michael Schmitt, the general editor of the two Tallinn Manuals, a secondary source of law cannot create law. States make laws.[60] New realities of the twenty-first century, including the COVID-19 pandemic, will catalyze the definition of rules of global digital cooperation architecture by states in the future.

At the regional level, the EU has demonstrated human-centered and risk-based approaches in the process of defining and implementing digital policy. The EU has created a strong legal basis for the protection of data and has generated standards that safeguard the right to privacy. The EU has also developed the ethical and legal frameworks for artificial intelligence with

the aim of protecting fundamental rights and establishing an institutional mechanism for avoiding the utilization of high-risk applications. As for the North Atlantic Alliance, ICTs have profoundly changed NATO's historical understanding of the core elements of collective defense. Historically, NATO focused on land, air, and naval defense capabilities. By recognizing cyberspace as an operational domain, the Allies have officially supported NATO's broader defense. Cyber defense continues to be integrated into the Alliance's operations and missions.

Ultimately, new technological advances, with their opportunities and challenges, will facilitate a dialogue among actors of the international community around a new international digital regime. This regime will define rules and impose responsibilities in the digital space. Responsible digital behaviors of state and non-state actors are preconditions for a stable and secure digital world. As a global actor, the UN should lead this process and enhance cooperation with regional organizations, including the EU and NATO. Furthermore, through sharing best practices, international actors should launch new joint digital projects for the promotion of world digital connectivity and the enhancement of digital capabilities, especially in developing countries. ***f***

ENDNOTES

1 International Digital Accountability Council, Digital Innovation and Democracy Initiative, "Rebuilding Trust in the Digital Ecosystem: New Mechanisms for Accountability," *The German Marshall Fund of the United States*, 2021, www.gmfus.org/news/rebuilding-trust-digital-ecosystem-new-mechanisms-accountability.
2 Virginia Bacay Watson, "The Fourth Industrial Revolution and its Discontents: Governance, Big Tech, and the Digitization of Geopolitics," in *Hindsight, Insight, Foresight: Thinking about Security in the Indo-Pacific,* ed. Alexander L. Vuving (Honolulu: Daniel K. Inouye Asia-Pacific Center for Security Studies, 2020), 37.
3 Ibid.
4 The United Nations, "Transforming our world: the 2030 Agenda for Sustainable Development," 2015, https://sdgs.un.org/2030agenda.
5 International Digital Accountability Council, "Rebuilding Trust."
6 Maciej Jarota, "Artificial intelligence and robotization in the EU - should we change OHS law?" *Journal of Occupational Medicine and Toxicology* 16 (18) (2021): 2.
7 International Institute for Applied Systems Analysis (IIASA), "Digitalization will transform the global economy," October 2018, 2.
8 Stefan Soesanto, "Europe's Digital Power: From Geo-Economics to Cybersecurity," *European Council on Foreign Relations*, April 18, 2017, 14.
9 Melissa Hathaway, "Patching Our Digital Future Is Unsustainable and Dangerous," *Centre for International Governance Innovation*, 2019, https://www.cigionline.org/articles/patching-our-digital-future-unsustainable-and-dangerous.
10 The United Nations Office of the Secretary-General's Envoy on Technology, "Implementing the Secretary-General's Roadmap for Digital Cooperation," April 2021, 1.

11 Ibid.
12 UN General Assembly (UNGA), "Roadmap for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation," Report of the Secretary-General 2020, 3.
13 Ibid., 6.
14 UN Envoy on Technology, "Implementing the Secretary-General's Roadmap," 2.
15 Ibid.
16 Ibid., 2-3.
17 UNGA, "Roadmap for digital cooperation," 8.
18 Ibid., 9.
19 Ibid., 10.
20 Lesley Swanson, "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict," *Loyola of Los Angeles International and Comparative Law Review* 32 (2010): 326.
21 Ibid, 327.
22 Ann Väljataga, "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly," *NATO Cooperative Cyber Defence Centre of Excellence,* September 1, 2017, https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html.
23 "UN GGE and UN OEWG," *GIP Digital Watch Observatory*, 2021, https://dig.watch/processes/un-gge#view-7541-1.
24 UN General Assembly, A/76/135, "Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security," July 14, 2021, 8.
25 "UN GGE and UN OEWG," *GIP Digital Watch Observatory*, 2021, https://dig.watch/processes/un-gge#view-7541-4.
26 "UN OEWG adopts its final report," *GIP Digital Watch Observatory*, March 12, 2021, https://dig.watch/updates/oewg-adopts-its-final-report.
27 Ibid.
28 UNGA, "Roadmap for digital cooperation," 15-16.
29 The United Nations, "High-Level Thematic Debate on Digital Cooperation and Connectivity: Whole-of-Society Responses to End the Digital Divide, April 27, 2021, and May 24, 2021, Summary of the President of the General Assembly," July 12, 2021, 3.
30 UNGA, "Roadmap for digital cooperation," 17.
31 Ibid.
32 Frances G. Burwell and Kenneth Propp, "The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?" *Atlantic Council,* issue brief, June 2020, 1.
33 Ibid., 2.
34 "2030 Digital Compass: the European way for the Digital Decade," *European Commission*, communiqué, March 9, 2021, 1.
35 Ibid, 2, 4.
36 Ibid., 5, 18.
37 Ibid., 18-19.
38 "Fostering a European approach to Artificial Intelligence," *European Commission*, communiqué, April 21, 2021, 1-2.
39 Ibid.
40 Ibid., 3.

41 "Ethics Guidelines for Trustworthy AI, High-Level Expert Group on Artificial Intelligence," *European Commission*, communiqué, April 8, 2019, 4.
42 Ibid.
43 Oliver Yaros, Ana Hadnes Bruder, Ondrej Hajda, and Ellie Graham, "The European Union proposes new legal framework for AI," *Mayer Brown*, May 5, 2021, https://www.mayerbrown.com/en/perspectives-events/publications/2021/05/the-european-union-proposes-new-legal-framework-for-artificial-intelligence.
44 Eve Gaumond, "Artificial Intelligence Act: What Is the European Approach for AI?," *Lawfare*, June 4, 2021, https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai.
45 Ibid.
46 "What is the GDPR? The EU's new data protection law?" *General Data Protection Regulation,* 2022, https://gdpr.eu/what-is-gdpr/.
47 Ibid.
48 "About ENISA – The European Union Agency for Cybersecurity," *European Union Agency for Cybersecurity*, https://www.enisa.europa.eu/about-enisa.
49 Ibid.
50 "NATO 2030: United for a New Era, Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary-General," *NATO,* report, November 25, 2020, 19.
51 Ibid., 45.
52 Jason Healey and Klara Tothova Jordan, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, Atlantic Council, September 2014: 2.
53 United States Senate, "Submitted Statement to the Senate Armed Services Committee on the FY 2017 Budget Request for the Department of Defense," statement of U.S. Secretary of Defense Ash Carter, March 17, 2016, https://www.armed-services.senate.gov/imo/media/doc/Carter_03-17-16.pdf.
54 Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?" *Stanford Law & Policy Review* 25 (Spring 2014): 270.
55 NATO, "Wales Summit Declaration," press release, September 4-5, 2014.
56 NATO, "Warsaw Summit Communiqué," press release, July 8-9, 2016.
57 "NATO and the European Union enhance cyber defense cooperation," *NATO*, February 10, 2016,
https://www.nato.int/cps/en/natohq/news_127836.html.
58 NATO, "NATO 2030," 45.
59 Keir Giles, Andrew Monaghan, *Legality in Cyber Space: An Adversary View* (Carlisle: U.S. Army War College Press, 2014): 9.
60 Michel Moutot, "'Tallinn Manual 2.0'—the rulebook for cyberwar" *Phys.org*, June 3, 2017, https://phys.org/news/2017-06-tallinn-manual-20the-rulebook-cyberwar.html.