



We support the Sustainable Development Goals



Digital Peace in Cyberspace:

An Invisible Pillar for the United Nations
Sustainable Development Goals

Authors

Jean-Yves Art

Daniel Akinmade Emejulu

Contributors

Ben Meany

John Hering

Nemanja Malisevic

Corporate, External, & Legal Affairs (CELA)
September 2020

Contents

4	Foreword
5	Executive summary
6	Introduction
8	I. Digital peace: What does it mean?
8	What is digital peace?
8	Why is it important?
9	What are cyberattacks? Whom do they harm?
12	Who are the actors behind cyberattacks?
13	Is there any link between non-state cyberattacks/cybercrime and state-led cyberattacks?
14	What are the current threat levels cyberattacks pose to the global economy?
16	II. Digital peace: An invisible pillar for the SDGs
16	Do cyberattacks threaten the Sustainable Development Goals?
17	Which SDGs are the most vulnerable to cyberattacks and risks?
18	Digital Peace and SDG 1: No Poverty
20	Digital Peace and SDG 3: Good Health and Well-Being
22	Digital Peace and SDG 6: Clean Water and Sanitation
24	Digital Peace and SDG 7: Affordable and Clean Energy
26	Digital Peace and SDG 8: Decent Work and Economic Growth
27	Digital Peace and SDG 9: Industry, Innovation and Infrastructure
29	Digital Peace and SDG 11: Sustainable Cities and Communities
31	Digital Peace and SDG 16: Peace, Justice and Strong Institutions
33	Digital Peace and SDG 17: Partnerships for the Goals
35	Shortlist of country positions on the policy link between cybersecurity and sustainable development
39	III. Global initiatives to sustain digital peace
39	Developing commitments for digital peace
39	United Nations (UN) working groups
42	United Nations policy frameworks
44	Private-sector approaches
45	Multistakeholder approaches
45	How does the Paris Call support the SDGs?
47	Why should governments universally commit to principles for digital peace in cyberspace?
50	Conclusion

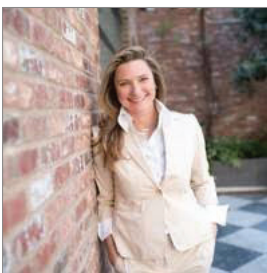
Foreword

Our digital world needs to be protected. Last year, nearly a billion people were victims of a cyberattack or digital crime. If you've not yet fallen victim to a digital attack, you probably know a victim of one. We know that nation-states are often behind the worst digital attacks against innocent people and the infrastructure that underpins societies—energy, transportation, healthcare, food, and water. A peaceful digital global society is something truly worth working to achieve, not least because virtually every digital attack ripples beyond its intended target and harms the lives of innocent citizens.

For example, the 2017 “WannaCry” attack—a true wake-up call—tore through cyberspace, hijacking more than 300,000 computers across 150 countries, including computers used by families, hospitals, governments, and businesses. WannaCry was followed closely by “NotPetya,” an attack estimated to have caused US\$10 billion in damage, ranging far beyond the initial targets in Ukraine. WannaCry and NotPetya were our wake-up moments—they raised an alarm. If we don't act now, global cyberattacks will continue to inflict grave economic harm and to risk human lives and well-being. More recently, the World Health Organization (WHO) and multiple healthcare sector organizations fell victim to targeted cyberattacks, which undermined their response efforts during the 2020 coronavirus pandemic.

At Microsoft, we're working to prevent digital attacks. We're not alone—others in industry and government have joined us in this effort. Now we need to amplify the protections in place and to cherish all that the digital world has given us by working for digital peace. So where do we go from here? We believe the answer lies in strong engagement from all stakeholders—including building resilience and security capacities, agreeing to norms of conduct and building the capacity to enforce them, or finding ways to address the challenges of attribution and deterrence. Cybersecurity concerns have escalated into one of the central security policy issues of our time, with serious implications for the stability of our economies and social structures.

To that end, we're pleased to present this paper, which makes the case that digital peace is part of a holistic approach needed to protect the social structures and physical infrastructure linked to the United Nations Sustainable Development Goals. Specifically, it encourages policymakers to consider cybersecurity principles that commit to digital peace worldwide as an invisible pillar, supporting the global goals in an increasingly digital world. We hope that policymakers consider this paper as a call to develop and evolve cybersecurity capacities and policies and to work toward a common approach that supports global alignment and coordination. We look forward to your feedback and continued partnership.



Kate O'Sullivan
General Manager, Digital Diplomacy
Corporate, External, & Legal Affairs (CELA)
Microsoft Corporation



John Frank
Vice President, United Nations Affairs
Corporate, External, & Legal Affairs (CELA)
Microsoft Corporation

Executive summary

It's time to strengthen principles committing to digital peace—the invisible pillar supporting the United Nations (UN) Sustainable Development Goals (SDGs). Like the pillars of global security, societal opportunity, and economic development, digital peace is a fundamental right in a modern world. The infrastructure required to meet the SDGs—universal electricity access, universal healthcare, and universal water access, for example—requires digital systems and tools. Digital peace is also needed to protect the functioning of governments, businesses, digital citizens, social structures, and critical infrastructure from cyberattacks.

Digital peace is a call for fundamental safeguards that protect people worldwide and sustain peaceful conditions for government and business operations. Cyberattacks increasingly threaten this peace. Even as governments make cybersecurity an ever-growing priority around the world, we believe that principles committing to digital peace in cyberspace need to be universal. Adopting norms and principles that commit to digital peace worldwide will protect the social structures and physical infrastructure linked to the Sustainable Development Goals and can help ensure their maintenance beyond the 2030 deadline. An alignment on cyber norms and principles is also critical to building global trust in the modern technologies needed to meet the goals in a digital-first world.

For example, consider good health and well-being, the third goal. Today, more than ever, we see how health emergencies, such as the coronavirus pandemic, pose a global risk. Yet cyberattacks threaten the safety of hospitals, medical facilities, government health agencies, and testing centers. Even the World Health Organization (WHO) has been subjected to a concerted range of cyberattacks during the pandemic. A universal commitment to principles for digital peace in cyberspace is needed to protect global health infrastructure. This same commitment is needed to protect other SDGs, as well.

Microsoft believes in a holistic approach to digital peace in cyberspace, based on principles and complementary norms that create universal protection. Digital peace requires cooperation across borders. It also requires an alignment on norms of conduct and enforcement strategies. Governments need to address the challenges of attribution and deterrence—particularly now, when malicious actors, including nation states, use cyberspace to inflict harm. Approaches to risk assessment and protection against cyber threats will differ as each nation develops its own cybersecurity strategy and framework, but these approaches must be complementary. Global principles committing to digital peace create the mechanisms that foster the cooperation needed to hold perpetrators of attacks accountable, build public trust, and maintain digital peace. They also advance capacity building for cyber policy and cyber practices.

We call on global policymakers and stakeholders to prioritize this invisible pillar and to strengthen principles for digital peace in cyberspace universally. Governments should work toward common norms and should implement global policies and principles that protect the social and physical investments needed to support the Sustainable Development Goals.

Based on following the policy landscape closely, Microsoft encourages stakeholders to work together through efforts such as the [Paris Call for Trust and Security in Cyberspace](#). This initiative recognizes the impact of cyberattacks on social, economic, and geopolitical fronts. As the primary global, multistakeholder, cybersecurity commitment at this time, the Paris Call offers the most digital protection for individuals and critical infrastructure at the core of the SDGs. Sustainability beyond 2030 requires a commitment to digital peace in cyberspace. Microsoft looks forward to your feedback and continued partnership.

Introduction

Around the world, stakeholders in government, business, and civil society are making crucial investments in infrastructure, human capital, development, and peace to achieve the **United Nations (UN) Sustainable Development Goals (SDGs)** and to deliver a more sustainable future by a deadline of 2030. The 17 global goals agreed upon by world leaders in 2015 address critical universal challenges, ranging from tackling inequality and the climate crisis to advancing energy access and peace and justice. Among those global priorities, peace is increasingly important in a world facing existential threats to international security—including dangers in the cyber risk landscape. Global commitments that address the myriad cyber risks to global peace, such as the Paris Call for Trust and Security in Cyberspace, recognize the impact of cyberattacks on social, economic, and geopolitical fronts. In a digital world, such global commitments protect and facilitate necessary investments in the UN global goals.

Peace is fundamental to the SDGs, especially considering the well-known challenges associated with achieving sustainable development in conflict contexts.¹ In addition to building peace in the physical world, building digital peace will safeguard the functioning of governments, businesses, digital citizens and systems, and critical infrastructure covered in the SDGs. The social structures and physical infrastructure at the heart of the SDGs require protection from paralyzing cyber threats and risks. Such protections must be universally strengthened to ensure that they truly sustain for the long term. For example, infrastructure-focused goals, such as universal electricity access, universal healthcare, universal water access, global technology cooperation, and safe transportation, all depend on digital systems and tools. As a result, cybersecurity principles that commit to digital peace worldwide will protect these classes of SDG infrastructure by limiting cyber disruptions that cripple economies. Likewise, cyber risks threaten the SDGs focused on improving social structures using technology, including financial inclusion, sustainable communities, effective institutions, participatory decision-making, and public access to information. Global commitments must also protect these social structures from cyberattacks to maintain peace. Such commitments also mitigate the risk of a global systems shutdown on the scale witnessed during the coronavirus pandemic in 2020.

To achieve and safeguard the SDGs, policymakers need a holistic approach, which includes the often overlooked cybersecurity component needed to safeguard the SDGs. Building resilience around the SDGs requires that policymakers assess and mitigate risks in cyberspace. Resilience also requires national capacity building for cyber policy and cyber practices. Policymakers need to mitigate the risks in cyberspace that can disrupt digital systems at the core of numerous SDGs—disruptions that effectively set back international investments in the global goals.

A resilient SDG agenda, therefore, relies on digital peace in three key respects. First, there's a need for principles committing to digital peace in cyberspace to become universal to sustain the social structures and infrastructure linked to the SDGs (beyond 2030)—for the digital and long-term future. Second, in the short term—between now and 2030—alignment on cyber principles is critical to building global trust in modern technologies, which are essential to delivering the SDGs in a digital-first world. Third, global principles on digital

¹ "UNDP offer on SDG implementation in fragile contexts," 2016. https://www.undp.org/content/dam/undp/library/SDGs/English/SDG_Implementation_in_Fragile_States.pdf

peace support international cooperation on technology and innovation, which is particularly necessary to meet SDG 17.² Technology cooperation across borders and promotion of technology access across regions of the world rely on collective trust that digital technology is inherently safe and not compromised by cyber risks. For example, developing countries, in particular, need to think about the inherent security of financial inclusion technology, and digital peace commitments mitigate the cyber risks that such technologies currently pose to people, banking systems, and government authorities—where digital capacity-building is in progress.

As such, the extent to which stakeholders commit to digital peace will build resilience around the SDGs and have profound effects on: (i) **sustaining** the social structures and infrastructure linked to the SDGs for the long term; (ii) **building** universal trust in technologies necessary to deliver the SDGs in a digital-first world; and (iii) **facilitating** global technology diffusion. Building this resilience around the SDGs relies on universal commitments to digital peace in cyberspace, ensuring a set of norms and principles that advance both international security and sustainable development.

This paper responds to three sets of questions that policymakers may have as they develop, evolve, and implement global commitments to digital peace in cyberspace to protect the UN SDGs and to ensure that the global goals take on digital resilience:

- **First**, questions about the necessity of digital peace. What is digital peace and what are cyberattacks? Who are the actors behind cyberattacks, and whom do they harm? What are the current threat levels that cyberattacks pose to the global economy? We consider these questions in the first section, “Digital peace: What does it mean?”
- **Second**, questions about the relationship between digital peace and the Sustainable Development Goals. Do cyberattacks threaten the SDGs? Which SDGs are the most vulnerable to cyberattacks, and how does digital peace in cyberspace protect the SDGs? We also discuss current efforts to protect social structures and infrastructure linked to the SDGs with effective cybersecurity principles and commitments. We consider these questions in the second section, “Digital peace: An invisible pillar for the SDGs.”
- **Third**, questions on the path toward a comprehensive digital peace commitment. What are the current international initiatives and commitments in place to advance digital peace? Why should governments build on best practice policies and universally commit to principles for digital peace in cyberspace, including to protect the SDGs? We consider these questions in the third section, “Global initiatives to sustain digital peace.”

² SDG 17 covers “Partnerships for the Goals.” It includes a call to strengthen the means of implementation and revitalize the global partnership for sustainable development. Specifically, SDG 17.6 sets for a target for “international cooperation on and access to science, technology and innovation,” including North-South and South-South cooperation.

I. Digital peace: What does it mean?

What is digital peace, and what are cyberattacks? Who are the actors behind cyberattacks, and who do they harm? Is there any link between non-state cyberattacks/cybercrime and state-led cyberattacks? What are the current threat levels cyberattacks pose to the global economy?

What is digital peace?

Digital peace is a call for the fundamental safeguards, which protect people worldwide and sustain peaceful conditions for government and business operations, to extend across digital technology worldwide. Now more than ever, technology is empowering people and organizations around the world. At the same time, it's also being progressively exploited by malicious actors that use cyberspace to inflict harm on people, social structures, and critical infrastructure. In 2014, the number of attempted cyberattacks was 20,000 a week. By 2017, that figure had risen to 600,000–700,000, according to Microsoft data.³ In 2019, global cyber incident costs reached a record high, with the average cost of a breach rising to US\$3.92 million and the biggest breaches topping US\$42 million.⁴ Given that people increasingly rely on online services and applications and that 77 percent of enterprises now have a portion of their computing infrastructure and data in the cloud,⁵ cyber risks extend to every digital citizen.

Why is it important?

The profile and range of malicious actors are also growing. Concerningly, governments are also behind cyberattacks, effectively using technology as a weapon against adversaries—even in times of peace. Although these attacks may start in the digital space, they can quickly spread to the physical world, where they have far-reaching impacts on economic, social, security, and geopolitical fronts. Conversely, geopolitical conflicts that exist in the physical world can also move to the digital world in the form of cyber conflicts and incidents. Universal principles on digital peace in cyberspace provide the necessary protection for people and global public goods, and they maintain truly peaceful conditions, which are currently being undermined by cyberattacks.

Recognizing the link between technology and the success of the **Sustainable Development Goals**, the United Nations recently affirmed that the internet can be a gateway to development and a means of implementation for many of the SDGs.⁶ However, the relationship between digital technology and the SDGs is only promising when there's collective trust in the safety and integrity of technology. In an increasingly digital-first world, where 5G, big data, and artificial intelligence are projected to rapidly accelerate goals ranging from education and healthcare,⁷ digital peace commitments underpin the technology for development nexus.

³ Cohen, Tova. "Microsoft to continue to invest over \$1 billion a year on cyber security," Reuters, January 26, 2017. <https://de.reuters.com/article/us-tech-cyber-microsoft/microsoft-to-continue-to-invest-over-1-billion-a-year-on-cyber-security-idUKKBN15A1GA>

⁴ Ponemon, Larry. "What's New in the 2019 Cost of a Data Breach Report," Security Intelligence, July 23, 2019. <https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report>

⁵ Columbus, Louis. "State Of Enterprise Cloud Computing, 2018," *Forbes*, August 30, 2018. <https://www.forbes.com/sites/louiscolombus/2018/08/30/state-of-enterprise-cloud-computing-2018/>

⁶ "UNDP offer on SDG implementation in fragile contexts," 2016. https://www.undp.org/content/dam/undp/library/SDGs/English/SDG_Implementation_in_Fragile_States.pdf

⁷ Lwanda, George. "How 5G can advance the SDGs," *World Economic Forum blog*, April 3, 2019. <https://www.weforum.org/agenda/2019/04/how-5g-can-advance-the-sdgs>

As the complexity of cyber risks continues to intensify, the SDGs' reliance on technology will face different risk scenarios and consequences, where principles for digital peace in cyberspace do not have universal strength.

What are cyberattacks? Whom do they harm?

The NATO-affiliated Tallinn Manual defines *cyberattack* as “a cyberoperation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”⁸ At a country level, the definitions of cyberattacks vary in national law, given that the threshold for causing “damage or destruction” may not always cover other problematic risks and ramifications. The UK National Cyber Security Centre (NCSC) defines cyberattacks as “malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices.”⁹ The NCSC defines cyber incidents as “a breach of a system’s security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems.”¹⁰

The Economist cites the first cyberattack to have occurred in 1834,¹¹ when the Blanc brothers introduced deliberate errors into a telegraph system in France to divert users and to gain financial market information more quickly. Since then, cyberattacks have matured in tandem with the evolution of technology, and the “modern first wave” of examples ranges from the first distributed denial-of-service (DDoS) cyberattack in 1988¹² to the cyberattacks in 2007 that affected public and financial systems in Estonia,¹³ showcasing the capacity for digital disruptions to cause harm to the real economy.

In the last decade, high-profile cyber incidents, such as Stuxnet in 2010, illustrated the security stakes of cybersecurity for physical infrastructure.¹⁴ Stuxnet was unlike any malicious computer virus or worm that came before it—rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak physical destruction on equipment in Iran’s nuclear program.¹⁵ Later in the same decade, cyberattacks broke into the mainstream news due in part to the foreign interference in the US presidential elections in 2016,¹⁶ which threatened established social structures. Less-reported incidents escalated cyber tensions in the 2010s, including the targeting of an Indian nuclear power plant in 2019.¹⁷

⁸ Schmitt, Michael N. (ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013: page 106, rule 30.

⁹ “NCSC glossary,” UK National Cyber Security Centre, January 5, 2018. <https://www.ncsc.gov.uk/information/ncsc-glossary>

¹⁰ “What is a cyber incident?” UK National Cyber Security Centre, November 15, 2018. [https://www.ncsc.gov.uk/information/what-cyber-incident#:~:text=The%20NCSC%20defines%20a%20cyber%20incident%20as%20a%20breach%20of,Computer%20Misuse%20Act%20\(1990\)](https://www.ncsc.gov.uk/information/what-cyber-incident#:~:text=The%20NCSC%20defines%20a%20cyber%20incident%20as%20a%20breach%20of,Computer%20Misuse%20Act%20(1990))

¹¹ Standage, Tom. “The crooked timber of humanity,” *The Economist*, October 5, 2017. <https://www.economist.com/1843/2017/10/05/the-crooked-timber-of-humanity>

¹² Shackelford, Scott. “What the world’s first cyber attack has taught us about cybersecurity,” *The World Economic Forum blog*, November 5, 2018. <https://www.weforum.org/agenda/2018/11/30-years-ago-the-world-s-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges/>

¹³ McGuinness, Damien. “How a cyber attack transformed Estonia,” BBC, April 27, 2017. <https://www.bbc.com/news/39655415>

¹⁴ Zetter, Kim. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon,” *Wired*, November 3, 2014. <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

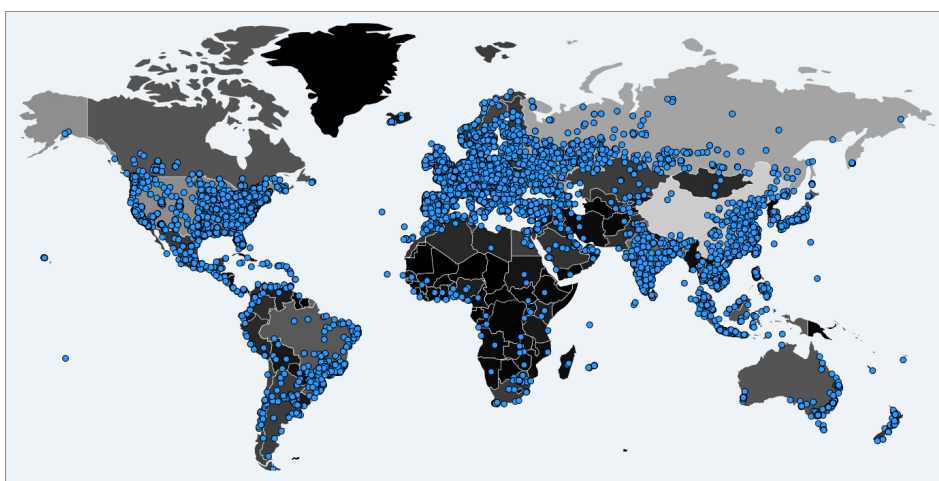
¹⁵ Ibid.

¹⁶ “Factbox: U.S. intel report on Russian cyberattacks in 2016 election,” Reuters, January 6, 2017. <https://www.reuters.com/article/us-usa-russia-cyber-intel-factbox/factbox-u-s-intel-report-on-russian-cyber-attacks-in-2016-election-idUSKBN14Q2HH>

¹⁷ Findlay, Stephanie, and Edward White. “India confirms cyber attack on nuclear power plant,” *Financial Times*, October 31, 2019. <https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6>

In the last three years, the world has reached an inflection point on the landscape of cyber risks. Among all categories of cyberattacks, state-led or state-sponsored cyberattacks, such as WannaCry and NotPetya in 2017, have seized the attention of policymakers across business, government, and civil society. At a juncture in time when people, data, and technology flow across borders and play an integral role in economic prosperity, limiting state-sponsored cyberattacks is especially critical to sustainable development, critical infrastructure, and national security. The spate of recent cases in 2017 confirms that state-sponsored cyberattacks severely threaten economies and serve as a cautionary tale for digitally safeguarding the social structures and infrastructure linked to the SDGs.

First, on May 12, 2017, the cyberattack which became known as **WannaCry** devastated the National Health Service (NHS)—the United Kingdom’s foremost healthcare provider. The cyberattack moved across UK hospitals, crashing computer systems, diverting ambulances, and shutting down lifesaving infrastructure and healthcare response capabilities. Notably, St. Bartholomew’s Hospital, which stayed open during World War II, was shut down by the WannaCry attack.¹⁸ Although the cyberattack started in the United Kingdom and Spain,^{19, 20} WannaCry rapidly spread to over 150 countries²¹ and, within hours, 300,000 computers in every corner of the globe were hit.²² The Microsoft Threat Intelligence Center (MSTIC) traced the WannaCry malware to a group called ZINC. Eventually, the United States, the United Kingdom, Australia, Canada, New Zealand, and Japan all attributed the WannaCry cyberattack to North Korea.²³



A world map shows where computers were infected by WannaCry, as recorded by MalwareTech.com.

¹⁸ St Bartholomew’s Hospital during World War Two,” BBC, December 19, 2005. <https://www.bbc.co.uk/history/ww2peopleswar/stories/10/a7884110.shtml>

¹⁹ Smith, Brad, and Carol Ann Browne. *Tools and Weapons – The Promise and Peril of the Digital Age*. Hodder & Stoughton, 2019: page 63.

²⁰ Cimpanu, Catalan. “Ransomware hits Spanish companies sparking WannaCry panic,” Zero Day, November 4, 2019. <https://www.zdnet.com/article/ransomware-hits-spanish-companies-sparking-wannacry-panic/>

²¹ Chappell, Bill. “WannaCry Ransomware: What We Know Monday,” NPR, May 15, 2017. <https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday>

²² Ibid.

²³ “White House Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea,” December 19, 2017. <https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>

Similarly, on June 27, 2017, the **NotPetya** cyberattack swept across the critical infrastructure of Ukraine, impacting an estimated 10 percent of all computers in the country—including a computer used at the Chernobyl cleanup site, north of Kyiv. NotPetya’s reach went beyond computers, also crippling businesses, transit systems, and banks in Ukraine. The attack moved past Ukraine’s borders, infiltrating multinationals, such as FedEx and Merck. Maersk, the Danish shipping giant, had its global computer network deeply corrupted.²⁴ Ultimately, the United States, the United Kingdom, Denmark, Lithuania, Estonia, Canada, and Australia attributed the NotPetya attack to Russia.²⁵ The following illustration points to a White House estimate, placing the financial losses from the attack at US\$10 billion.

The Cost of NotPetya

In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Here’s a list of the approximate damages reported by some of the worm’s biggest victims.

\$870,000,000

Pharmaceutical company Merck

\$400,000,000

Delivery company FedEx (through European subsidiary TNT Express)

\$384,000,000

French construction company Saint-Gobain

\$300,000,000

Danish shipping company Maersk

\$188,000,000

Snack company Mondelez (parent company of Nabisco and Cadbury)

\$129,000,000

British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)

\$10 billion

Total damages from NotPetya, as estimated by the White House

Source: (Greenberg, 2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History in *Wired*

By late March 2020, amid the coronavirus pandemic, the United Nations warned that cyber actors are exploiting the COVID-19 crisis—from the proliferation of false information about the virus and the sales of fake coronavirus cures online to cyberattacks on hospitals’ critical information systems.²⁶ In May 2020, over 40 leaders—ranging from former heads of state to private sector executives and Nobel laureates—signed a [letter calling on international governments and the United Nations to help prevent the cyberattacks](#) that have plagued healthcare and research facilities during the coronavirus crisis, disrupting their ability to operate when vitally needed.²⁷

Beyond the cyberattacks disrupting the healthcare and humanitarian systems amid the pandemic, the broader cyber risk landscape heightened during the pandemic 2020, affecting a diverse range of organizations. Microsoft observed COVID-19–themed attacks peak in the

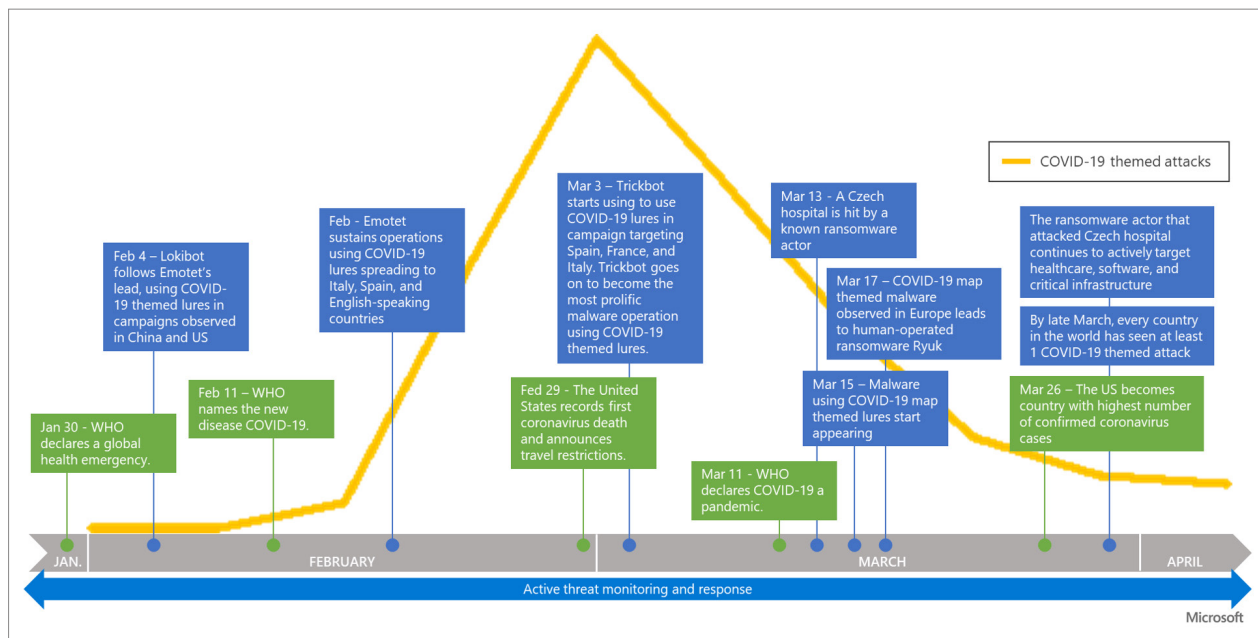
²⁴ Greenberg, Andy. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired*, August 22, 2018. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

²⁵ Charlet, Kate. “How the U.S. Approach to Cyber Conflict Evolved in 2018—and What Could Come Next,” *World Politics Review*, December 26, 2018. <https://www.worldpoliticsreview.com/articles/27071/how-the-u-s-approach-to-cyber-conflict-evolved-in-2018-and-what-could-come-next>

²⁶ “UN tackles ‘infodemic’ of misinformation and cybercrime in COVID-19 crisis,” United Nations Department of Global Communications, March 31, 2020.” <https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19>

²⁷ “A Call to All Governments: Work Together Now to Stop Cyberattacks on the Healthcare Sector,” CyberPeace Institute, May 26, 2020. <https://cyberpeaceinstitute.org/campaign/call-for-government>

first two weeks of March,²⁸ which coincided with many nations beginning to take action to reduce the spread of the virus and with travel restrictions coming into effect.²⁹ By the end of March 2020, every country in the world had seen at least one COVID-19-themed attack.³⁰



Who are the actors behind cyberattacks?

The actors behind cyberattacks vary in their profiles, intentions, and geographies. In most cases, cyberattacks can be connected to one of the following six actors: corporate competitors, hacktivists, organized criminal groups, opportunists, company insiders, or nation-states.³¹ On the geopolitical front, 60 states already have or are developing cyber offensive capabilities.³² A report published by the Italian Centre on Cybersecurity at the Institute for International Political Studies (ISPI) argues that every state uses cyberspace to protect and advance its national interests in the global cyber arena.³³ However, the ISPI also observes that four countries—Russia, North Korea, China, and Iran—“stand out because they all appear as having elected cyberspace the ‘domain of choice’ to pursue their geo-strategic objectives, with campaigns that fall below some interpretations of ‘use of force,’ while also offering the semblance of level of plausible deniability.”³⁴ Plausible deniability is giving way to improving attribution capabilities, which are increasingly able to ascribe cyberattacks with “high confidence.”³⁵

²⁸ Microsoft Threat Protection Intelligence Team. “Exploiting a crisis: How cybercriminals behaved during the outbreak,” June 16, 2020. <https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/>

²⁹ “Joint ICAO-WHO Statement on COVID-19,” March 11, 2020. <https://www.who.int/news-room/articles-detail/joint-icao-who-statement-on-covid-19>

³⁰ Microsoft Threat Protection Intelligence Team. “Exploiting a crisis: How cybercriminals behaved during the outbreak,” June 16, 2020. <https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/>

³¹ The Council of Economic Advisers, White House. “The Cost of Malicious Cyber Activity to the U.S. Economy,” February 2018. <https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>

³² Valentino-DeVries, Jennifer, and Danny Yadron. “Cataloging the World’s Cyberforces,” *The Wall Street Journal*, October 11, 2015. <https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710>

³³ Massolo, Giampiero. “Confronting an ‘Axis of Cyber’?” ISPI online, October 2018. https://www.ispionline.it/sites/default/files/pubblicazioni/cyber_def_web2.pdf

³⁴ Rugge, Fabio (ed.). “Confronting an ‘Axis of Cyber’?” ISPI online, October 2018. https://www.ispionline.it/sites/default/files/pubblicazioni/cyber_def_web2.pdf

³⁵ Repussard, Eva-Nour. “There Is No Attribution Problem, Only a Diplomatic One,” *E-International Relations*, March 22, 2020. <https://www.e-ir.info/pdf/82357>

It's worth elaborating on the profiles of the broad categories of cyberattackers mentioned earlier, as identified by the White House Council of Economic Advisers.³⁶ *Corporate competitors* use cyberattacks to gain information on their competitors, ranging from financial and strategic to workforce-related information. *Hactivists* predominantly use cyberattacks for political agendas or to establish an ideological position. Hactivists tend to be individuals or private groups. *Organized criminal groups* mostly use cyberattacks for criminal activities or profit-seeking. For example, these groups stage disruptive cyberattacks on public and private entities for ransom or to steal personally identifiable information (PII) to sell on the dark web. *Opportunists* typically attack organizations using widely available codes and techniques and, thus, usually represent the least advanced form of adversary. Opportunists are usually amateur hackers driven by a desire for notoriety. Another class of cyberattacks relies on former or disgruntled *company insiders* looking for revenge or financial gain. Given their vast resources and growing offensive capabilities, *state-sponsored* cyberattacks pose unique threats to global public goods.

Is there any link between non-state cyberattacks/cybercrime and state-led cyberattacks?

It is useful to consider this point in the context of the categories of cyberattackers identified by the White House Council of Economic Advisers.³⁷ Putting aside the state-led or sponsored category of cyberattackers, the five additional categories identified are corporate competitors, hactivists, organized criminal groups, opportunists, and company insiders. Although each group may operate as a private party when launching cyberattacks, these malicious actors can also be utilized or backed by nation-states.³⁸ The Council on Foreign Relations refers to this concept as the "Blurred Lines"³⁹ phenomenon—where non-state actors and state actors can create overlaps in their cyber offensive actions, citing the APT17 and APR41 groups as examples of a non-state actor being held responsible for launching privately run cyberattacks, cyberattacks linked to the Chinese government, and cyberattacks affecting the Chinese citizens.⁴⁰

Methods used in cybercrimes by non-state actors can also be emulated by state actors, typically at a grand scale, with far-reaching geopolitical implications. The WannaCry cyberattack in 2017 famously utilized *ransomware*—malicious software that demands that a fee is paid before permitting a system to work again. At a time characterized by heightening geopolitical tensions, state-sponsored cyberattacks are considered as a low-cost tool of statecraft which serves political, economic, technical, and military agendas.⁴¹ Cyberattacks offer these national agendas extraordinary offensive capabilities, given their special ability

³⁶ The Council of Economic Advisers, White House. "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018. <https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>

³⁷ Ibid.

³⁸ "Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar," Public-Private Analytic Exchange, 2019: page 3. https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf

³⁹ Merrigan, Elizabeth. "Blurred Lines Between State and Non-State Actors," Council on Foreign Relations blog, December 5, 2019. <https://www.cfr.org/blog/blurred-lines-between-state-and-non-state-actors>

⁴⁰ Ibid.

⁴¹ Coats, Daniel R. "Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community," Office of the Director of National Intelligence, February 13, 2018. <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA--Unclassified-SSCI.pdf>

to cripple water, electricity, financial, and banking systems from a distance. Although state-sponsored cyberattacks are the priority risk to mitigate for the SDGs, cyberattacks emanating from non-state actors can be significantly related.

To limit the cyber risks threatening social structures and infrastructure linked to the SDGs, a holistic approach therefore must also include measures to tackle cybercrime in legal systems around the world. Governments stand to gain from capacity building on cyber policy and cyber practices. Strengthening cybercrime prevention and prioritizing the effective prosecution of cybercriminals reduces the risk of creating “safe spaces” for cyber risks to thrive. The private sector and civil society organizations must play a constructive role to help governments build their capacity to identify and tackle cyber risks. At a multilateral level, the United Nations Office on Drugs and Crime (UNODC) runs a [Global Programme on Cybercrime](#), which provides focused technical assistance for capacity building, prevention and awareness-raising, international cooperation, and analysis on the phenomenon, principally in developing countries.

What are the current threat levels cyberattacks pose to the global economy?

More than 60 states already have or are developing cyber offensive capabilities.⁴² Cyberattacks are considered “the perfect crime,” due to the perceived anonymity and lack of accountability they afford users. Taken together, these factors also create a special class of risk to the global economy. In *Tools and Weapons: The Promise and Peril of the Digital Age* (2019), Brad Smith and Carol Ann Browne highlight the risks of cyberattack in a future characterized by smart cities (SDG 11): “If a city loses its electricity, telephones, gas lines, water system and internet, it can be thrown back into something that feels like the Stone Age. If it’s winter, people may freeze. If it’s summer, people may overheat. Those who rely on medical devices may lose their lives.” To what extent are stakeholders protecting the global economy from the perfect crime?

Cyberattacks pose an existential threat to a sustainable development agenda predicated on technology and digital systems, specifically an incoming generation of technology characterized by hyperconnectivity, artificial intelligence (AI), the Internet of Things (IoT), and 5G—where cyber risks will affect both the underlying technology and the real-world infrastructure it controls. In the United States alone, malicious cyber activity cost the US economy between US\$57 billion and US\$109 billion in 2016.⁴³ Estimating the economic cost of cyberattacks at a global level requires an extrapolation of such figures by several orders of magnitude. A study by the Atlantic Council and Zurich Insurance Group attempts to estimate these global costs within the timeline of the SDGs.⁴⁴ It offers a best-case scenario, termed “Cyber Shangri-La,” in which technology booms are driven by strong cybersecurity. In this scenario, the recurring annual economic benefits result in a cumulative net global gain of **US\$190 trillion** by the year 2030—about US\$30 trillion higher than that of the base case, a projection based on business as usual.

⁴² Valentino-DeVries, Jennifer, and Danny Yadron. “Cataloging the World’s Cyberforces,” *The Wall Street Journal*, October 11, 2015. <https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710>

⁴³ The Council of Economic Advisers, White House. “The Cost of Malicious Cyber Activity to the U.S. Economy,” February 2018. <https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>

⁴⁴ “Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures,” Zurich Insurance Group and the Atlantic Council’s Brent Scowcroft Center on International Security, 2015. <https://publications.atlanticcouncil.org/cyber risks/risk-nexus-september-2015-overcome-by-cyber-risks.pdf>

In the worst-case scenario, which it terms “Clockwork Orange Internet,” perpetual cyber warfare ultimately creates a negative impact on the internet and economic growth. In this scenario, the world loses nearly **US\$90 trillion** of potential net economic benefit by 2030. These varied risk scenarios benefit from effective mitigation from policymakers, including global commitments to digital peace in cyberspace.

Finally, a United Nations Economic and Social Council (ECOSOC) statement affirms that “cyberattacks have the potential for triggering inter-State and other conflicts which can put the entire development process at considerable risk.”⁴⁵ This risk is exacerbated when we consider that hostile states are becoming more aggressive in their behavior. According to the UK’s 2018 Joint Select Committee on National Security Strategy, states still represent the most acute and direct cyber threat, and some states are exploring ways of disrupting critical national infrastructure.⁴⁶

⁴⁵ Statement by H.E. Mr. Lazarous Kapambwe, President of ECOSOC. “Special Event on Cybersecurity and Development,” December 9, 2011. https://www.un.org/en/ecosoc/president/statement_2011/statement_ecosoc_president_opening_remark-9_dec_2011.pdf

⁴⁶ “Protecting CNI against cyber attack: a ‘wicked’ problem,” Cyber Security of the UK’s Critical National Infrastructure, 2018. <https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/170805.htm>

II. Digital peace: An invisible pillar for the SDGs

Do cyberattacks threaten the Sustainable Development Goals? Which SDGs are the most vulnerable to cyberattacks? How does digital peace in cyberspace protect the SDGs? What are the current commitments in place to protect social structures and infrastructure, which are linked to the SDGs?

Do cyberattacks threaten the Sustainable Development Goals?

The WannaCry and NotPetya attacks signal an escalation in government cyber offensive capabilities. Citizens, technology users, public entities, civil society, and corporations have all become significantly affected by the effects of these destructive digital disruptions. A latent concern is the potential for an escalation in government versus government cyberattacks. The WannaCry attack affected government institutions around the world, ranging from the United Kingdom⁴⁷ and India⁴⁸ to Brazil,⁴⁹ China,⁵⁰ and Russia.⁵¹ The Sustainable Development Goals were adopted by states, which themselves must observe digital peace to safeguard and sustain development within their borders. This is especially critical as the United Nations calls for Member States and stakeholders to mobilize and increase investments for SDGs infrastructure,⁵² which—without global commitments to digital peace—remains vulnerable to offensive and retaliatory cyberattacks.

On the business front, WannaCry illustrates that cyberattacks spontaneously disrupt myriad systems, including banking, education, energy, health, manufacturing, telecommunications, and transportation, all of which hold special significance to the achievement of the SDGs in a digital-first world. Where digital peace does not exist and cyberattacks grow in scale and frequency, the social structures and infrastructure covered in the SDGs will remain inescapable victims—casting doubt on the success of numerous SDG targets.

The New Climate Economy Report suggests that US\$90 trillion investment is needed by 2030 for infrastructure,⁵³ which includes “everything from energy to public transport, buildings, water supply, and sanitation.” Where digital peace commitments are not universally adopted,

⁴⁷ “Investigation: WannaCry cyber attack and the NHS,” Report by the Comptroller and Auditor General, April 25, 2018: pages 11–15. <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>

⁴⁸ “WannaCry did hit India and even central govt portal. So why did Centre downplay the ransomware attack?” *India Today*, June 19, 2017. <https://www.indiatoday.in/mail-today/story/ransomware-wannacry-cyberattack-global-ransomware-attack-india-983427-2017-06-19>

⁴⁹ “WannaCry Ransomware Attack Summary,” Data Protection Report, May 17, 2017. <https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/>

⁵⁰ Lau, Mimi. “Chinese police and petrol stations hit by ransomware attack,” *South China Morning Post*, May 14, 2017. <https://www.scmp.com/news/china/society/article/2094291/chinese-police-and-petrol-stations-hit-ransomware-attack>

⁵¹ Winsor, Morgan, et al., “Researcher ‘accidentally’ stops spread of ‘unprecedented’ global cyberattack,” ABC News, May 13, 2017. <https://abcnews.go.com/International/researcher-accidentally-stops-spread-unprecedented-global-cyberattack/story?id=47390745>

⁵² “More Money Needed to Implement Sustainable Development Goals, Secretary-General Tells ECOSOC Financing for Development Forum, Calling 2019 ‘Defining Year,’” United Nations Secretary General press release, April 15, 2019. <https://www.un.org/press/en/2019/sgsm19546.doc.htm>

⁵³ “The Sustainable Infrastructure Imperative: Financing For Better Growth And Development,” The New Climate Economy: The Global Commission on Climate and the Economy, 2016. <https://www.un.org/pga/71/wp-content/uploads/sites/40/2017/02/New-Climate-Economy-Report-2016-Executive-Summary.pdf>

businesses working toward the sustainable development agenda risk facing avoidable investment setbacks from attacks that effectively reverse the quantum of capital flows poured into the sustainable development agenda.

Which SDGs are the most vulnerable to cyberattacks and risks?

A second key step for policymakers as they build global commitments for digital peace in cyberspace is to consider the importance of digital peace in cyberspace to specific Sustainable Development Goals. At some level, cybersecurity is crucial to achieving all the SDGs, considering the reliance on digital infrastructure and systems to develop, implement, monitor, and collaborate on the goals across borders. The importance of building resilience around the social structures and infrastructure in the SDGs requires policymakers to assess how risks in cyberspace create vulnerabilities for specific global goals. This risk appreciation is needed to mitigate such risks with commitments to ensure digital peace.

This section highlights the importance of digital peace to the individual UN global goals. Although cyberattacks pose varying levels of risk to the implementation of all 17 Sustainable Development Goals, the following global goals are some examples that particularly highlight the risks of state-sponsored cyberattacks to individual SDGs:

- SDG 1: No Poverty ([page 18](#))
- SDG 3: Good Health and Well-Being ([page 20](#))
- SDG 6: Clean Water and Sanitation ([page 22](#))
- SDG 7: Affordable and Clean Energy ([page 24](#))
- SDG 8: Decent Work and Economic Growth ([page 26](#))
- SDG 9: Industry, Innovation and Infrastructure ([page 27](#))
- SDG 11: Sustainable Cities and Communities ([page 29](#))
- SDG 16: Peace, Justice and Strong Institutions ([page 31](#))
- SDG 17: Partnerships for the Goals ([page 33](#))

Digital Peace and SDG 1: No Poverty



This Sustainable Development Goal aims to reduce the people living in poverty by half in the next 10 years. Specifically, target 1.4 works toward this intention with a call for all men and women—in particular, the poor and the vulnerable—to have equal rights to economic resources and to appropriate new technology and financial services.

For the technology and financial inclusion portions, the UN High-level Panel on Digital Cooperation laid out careful recommendations in its 2019 report, [The Age of Digital Interdependence](#), including “Leaving No One Behind.” According to the report, digital technologies will only help progress toward the full sweep of the SDGs if policymakers think more broadly than the important issue of access to the internet and digital technologies. It goes on to state, “Access is a necessary, but insufficient, step forward. To capture the power of digital technologies we need to cooperate on the broader ecosystems that enable digital technologies to be used in an inclusive manner.” In other words, the promise of technology to create financial inclusion and alleviate poverty requires both technology access and broad inclusivity.

Importantly, cyber risks that threaten both access and inclusivity to new technology must be mitigated to achieve target 1.4. Similarly, target 1.5 recognizes a need for policymakers to reduce the susceptibility of the poor and other vulnerable populations to economic, social, and environmental shocks and disasters. Cyber risks constitute an economic and social threat capable of undermining the poverty reduction goal. Poor and vulnerable populations increasingly depend on the internet for information, financial services, and economic participation. In 2019, the World Economic Forum’s [Global Risk Report](#) cited cyberattacks among its top 10 global risks of highest concern, highlighting the special vulnerabilities between technology and infrastructure development.

CASE IN POINT

According to *Forbes*, a 2015 cyberattack on the Central Bank of Bangladesh was linked to North Korean hackers, who made off with US\$81 million. In 2018, India’s Cosmos Bank was hacked to the tune of US\$13.5 million. In 2019, those same hackers infiltrated the Bank of Chile’s ATM network and siphoned off \$10 million. In the case of Cosmos Bank in India, breaches affecting a cooperative bank serving key demographics breach public trust and confidence, which is pivotal to the financial inclusion goals in SDG 1.

For vulnerable populations increasingly seeking technological access and inclusion, universal principles committing to digital peace reduces the risks that cyberattacks pose to everyday people. The prevalence of identity theft, data exfiltration, and online fraud schemes undermine target 1.4, specifically as governments roll out digital efforts for financial inclusion and microfinance. Although these cybercrimes are often carried out by non-state actors, identity theft and data exfiltration could be inflicted by states that use cyberspace as a tool of statecraft to cause civic disruption in targeted locations.

The digital landscape in developing countries is particularly vulnerable to cyberattacks. Weak cybersecurity defensive capability, the shortage of skilled personnel, and the fledgling regulatory landscapes all create an environment particularly vulnerable to cyberattacks from both state and non-state actors. The task of target 1.4 is to provide the poor and the vulnerable

with rights to economic resources and to appropriate new technology. To provide this technology at scale, the digital space must be secure from cyberattacks to inspire trust and the widespread adoption of digital technologies.

In Africa alone, an estimated US\$3.5 billion was lost to cybercrime in 2017,⁵⁴ affecting businesses, individuals, families, financial institutions, and government agencies. However, these vulnerabilities to incidents of cybercrime also expose the susceptibility of developing countries to state-sponsored cyberattacks. Principles committing to digital peace in cyberspace worldwide will support the diffusion of safe technology to promote inclusion and reverse poverty.

⁵⁴ Dahir, Adbi Latif, "Cybercrime is costing Africa's businesses billions," Quartz Africa, June 12, 2018. <https://qz.com/africa/1303532/cybercrime-costs-businesses-in-kenya-south-africa-nigeria-billions/>

Digital Peace and SDG 3: Good Health and Well-Being



This Sustainable Development Goal aims to achieve universal healthcare coverage in the next 10 years. Specifically, target 3.8 states this objective as delivering access to “quality essential health-care services and access to **safe**, effective, quality and affordable essential medicines.” The healthcare sector is increasingly embracing digital technology, and the value of the global digital health market is estimated to reach

US\$234 billion by 2023.⁵⁵

Cyber risks threaten the safety of medical infrastructure in a universal healthcare system, which is heavily and increasingly reliant on digital technologies. In March 2020 alone, amid global response efforts to the coronavirus pandemic, hospitals, medical facilities, government health agencies, testing centers—and even the World Health Organization (WHO)—faced targeted cyberattacks perpetrated by malicious actors.⁵⁶ Numerous countries have been linked to the cyber offensive actions undermining the fight against the coronavirus, spreading disinformation, and working to gain access to US and WHO servers.⁵⁷

The International Criminal Police Organization (INTERPOL) detected a significant increase in cyberattacks against hospitals around the world that are engaged in the COVID-19 response⁵⁸—attacks that could directly lead to deaths in cases where medical devices are compromised. To support global efforts against this critical danger, INTERPOL has issued a Purple Notice alerting police in all its 194 member countries to the heightened threat.⁵⁹

Recognizing the need for states to act to protect individuals and infrastructure, including in global emergencies, the International Committee of the Red Cross (ICRC) has proposed a norm prohibiting

CASE IN POINT

According to **WHO**, cyberattacks have increased fivefold since the start of the coronavirus pandemic in 2020. They range from ransomware operations, aimed at crippling primary and urgent care networks in exchange for payouts, to disinformation campaigns aimed at undermining and disrupting wider elements of the response to the pandemic, including testing and vaccine research facilities. In May 2020, ICRC President Peter Maurer and Microsoft President Brad Smith added their names to a **list of more than 40 international leaders** calling on the world’s governments to take immediate and decisive action to prevent and stop cyberattacks on the health sector amid the pandemic.

⁵⁵ “Global digital healthcare market to surpass \$234.5bn by 2023,” Health Europa EU, October 11, 2019. <https://www.health.europa.eu/digital-healthcare-market-234-5bn-2023/94032/>

⁵⁶ Ruhl, Christian. “Note to Nations: Stop Hacking Hospitals,” Foreign Policy, April 6, 2020. <https://foreignpolicy.com/2020/04/06/coronavirus-cyberattack-stop-hacking-hospitals-cyber-norms/>

⁵⁷ Ibid. and Joseph Menn et al. “Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus – sources,” Reuters, April 2, 2020. <https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC>

⁵⁸ “Cybercriminals targeting critical healthcare institutions with ransomware,” Interpol, April 4, 2020. <https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware>

⁵⁹ Ibid.

states from conducting or knowingly supporting information and communications technology (ICT) activity that would harm medical services or medical facilities and would oblige them to take measures to protect medical services from harm.⁶⁰

These protections would significantly build resilience around goal 3 and protect all stakeholder investments, including in a context where digital-first healthcare is here to remain.

Beyond cyber risks to infrastructure and devices, healthcare data is also extremely valuable at a country and an industry level. Accenture reports that cybercrime in the healthcare industry is above the averages found in other industries, with an average annualized cost of US\$12.47 million.⁶¹ Total healthcare breaches were estimated to cost the sector US\$4 billion in 2019.⁶²

In addition to protecting people covered in the universal healthcare coverage ambition, target 3.D aims to strengthen the capacity of all countries, “in particular developing countries, for early warning, risk reduction and management of national and global health risks.” To safeguard the universal healthcare system of the twenty-first century, universal support for norms and principles committing to digital peace in cyberspace is necessary to protect increasingly digital medical infrastructure, services, and tools—some of which live in our bodies.

⁶⁰ “Norms for responsible State behavior on cyber operations should build on international law,” ICRC Statement, February 11, 2020. <https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law>

⁶¹ Ibid.

⁶² “Healthcare Data Breaches Costs Industry \$4 Billion by Year’s End, 2020 Will Be Worse Reports New Black Book Survey,” Black Book Market Research, November 4, 2019. <https://www.prnewswire.com/news-releases/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-will-be-worse-reports-new-black-book-survey-300950388.html>

Digital Peace and SDG 6: Clean Water and Sanitation



This Sustainable Development Goal aims to achieve universal and equitable access to safe and affordable drinking water for all—in the next 10 years. Today, 3 in 10 people lack access to safe drinking water services, and 6 in 10 lack access to safe sanitation facilities. Technology will be central to solving water efficiency challenges. Specifically, target 6.5 calls for the implementation of integrated global water resources management at all levels, by 2030, “including through transboundary cooperation, as appropriate.” In other words, to solve water scarcity, which affects over 40 percent of the global population, transboundary water cooperation and water security will be required.

In the pursuit of the goals for universal water access and transboundary cooperation, global water system infrastructure bears the risks of cyberattacks, which specifically threaten supervisory control and data acquisition (SCADA) systems. Universally supported norms and principles committing to digital peace in cyberspace mitigate the risks of hackers remotely seizing control and operation of water pumps, valves, and hydrants or of providing incorrect operational details to compromise water quality. These cyber risks, if realized, could harm or kill people, set back investments in water, and create volatile economic and social conditions driven by water insecurity.

More recently, in May 2020, Israel’s cyber defense agency confirmed a cyberattack that targeted water and sewage treatment facilities around the country.⁶³ Its suspected goal was to trick the computers into increasing the amount of chlorine added to the treated water that flows to Israeli homes.⁶⁴ Around this same time, a cyberattack also targeted the computer systems at Iran’s busiest hub for maritime trade, Shahid Rajaei Port in Bandar Abbas, near the Strait of Hormuz.⁶⁵ According to Iran’s Ports and Maritime Organization, the attack disrupted private operating companies’ systems for several hours.⁶⁶ These cases illustrate the cyber vulnerabilities in water systems and the transboundary cooperation systems, both of which are essential to target 6.5.

CASE IN POINT

In 2016, shortly after the SDGs were adopted, a group of hackers broke into a public utility water treatment system and changed the levels of chemicals being used to treat tap water. Infiltrating the water system server gave the attackers the ability to manipulate controls and tamper with water valves, chemical mixtures, and water flow. The attack is referred to as the **Kemuri Water Company (KWC)** because a telecommunications company which studied the event is not releasing the name of the affected water company or the country in which it operates, partly due to the sensitive nature of the breach, which gave the hackers personal and financial data records of 2.5 million customers.

⁶³ Brennan David. “Iran Explosions: The Main Suspects,” *Newsweek*, July 13, 2020. <https://www.newsweek.com/iran-explosions-main-suspects-natanz-sabotage-israel-us-homeland-cheetahs-1517321>

⁶⁴ Arivastava, Mehul. “Israel-Iran attacks: ‘Cyber winter is coming,’” *Financial Times*, May 31, 2020. <https://www.ft.com/content/3ea57426-40e2-42da-9e2c-97b0e39dd967>

⁶⁵ Baram, Gil, and Kevin Lim. “Israel and Iran Just Showed Us the Future of Cyberwar with Their Unusual Attacks,” *Foreign Policy*, June 5, 2020. <https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/>

⁶⁶ Ibid.

The cyber risks threatening goal 6 are already being mitigated at a country and sub-national level. Following recent attacks in Colorado and New York water systems, including one suspected to come from Iran,⁶⁷ the US Congress passed the [Water Infrastructure Act \(2018\)](#), requiring large-scale water systems to provide risk resilience and emergency response plans that address both physical and cybersecurity threats. Universal support for principles committing to digital peace in cyberspace also protects water systems and infrastructure, which, in turn, secures the availability and sustainable management of water for all people—in line with goal 6.

⁶⁷ Sobczak, Blake. "Hackers force utilities to sink or swim," E&E News, March 28, 2019. <https://www.eenews.net/stories/1060131769>

Digital Peace and SDG 7: Affordable and Clean Energy



This Sustainable Development Goal aims to achieve universal access to affordable, reliable, and modern energy services for all—in the next 10 years. Notably, in target 7.B, the UN sets an objective to **expand infrastructure and upgrade technology** for supplying modern and sustainable energy services for all in developing countries by 2030.

The target makes a special reference for the urgency of energy infrastructure to be upgraded in developing countries. These technological upgrades require thoughtful mitigation against cybersecurity risks, which disrupt energy access for all.

In December 2015, three months after the SDGs were adopted, Ukraine became victim to the first known successful cyberattack on an electronic grid.⁶⁸ The perpetrators gained access to all the affected energy distribution company systems more than six months before the outage that temporarily left about 225,000 customers without power.⁶⁹ Two years later, in 2017, Ukraine's energy grid was targeted in another cyberattack which caused power outages in Kyiv.⁷⁰

In all parts of the world, developed and developing, critical national infrastructure (CNI) has often been built without cybersecurity in mind. Recognizing this vulnerability, the energy utility industry is forecasted to invest US\$1.7 billion in protecting energy systems against cyberattacks.⁷¹

Cyberattacks on electrical grids will have dramatic spillover effects on power-dependent infrastructure, ranging from airports and lifesaving devices in hospitals to advanced manufacturing and food production systems. In countries most vulnerable to cyberattacks, disruptions will set back the clock on their development progress, contrary to the objectives set out in target 7.B.

CASE IN POINT

The **Council on Foreign Relations** reported that in 2014, Admiral Michael Rogers, US director of the National Security Agency, testified before the US Congress that China and a few other countries likely had the capability to shut down the US power grid. Iran, as an emergent cyber actor, could acquire such capability. More recently, in May 2020, the **Center for Strategic and International Studies (CSIS)** reported that German officials found that a Russian hacking group associated with the FSB had compromised the networks of energy, water, and power companies in Germany by exploiting IT supply chains.

⁶⁸ Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

⁶⁹ Polityuk, Pavel, et al. "Ukraine's power outage was a cyber attack: Ukrenergo," Reuters, January 18, 2017. <https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA>

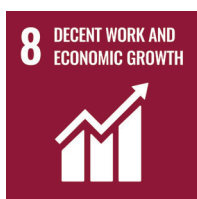
⁷⁰ Ibid.

⁷¹ "Grid automation drives increase in utility cybersecurity investments – report," Smart Energy International, August 10, 2017. <https://www.smart-energy.com/industry-sectors/smart-grid/cybersecurity-technologies-navigant-research/>

Recognizing the threat to such geopolitically sensitive systems, the European Union and its member states recently underlined the severity of threats against critical infrastructure, stating that “critical infrastructures are no longer confined to the borders of States but are increasingly becoming transnational and interdependent; the scale of the threat remains a major concern. Therefore, the protection of critical infrastructure is of such importance.”⁷² Digital peace norms and principles are needed to mitigate cyber risks threatening the digital technology necessary for supplying modern and sustainable energy services for all.

⁷² Joint comments from the EU and its member states on the initial ‘pre-draft’ report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security. <https://front.un-arm.org/wp-content/uploads/2020/05/eu-contribution-alignments-owwg.pdf>

Digital Peace and SDG 8: Decent Work and Economic Growth



This Sustainable Development Goal aims to promote sustained, inclusive, and sustainable economic growth, in addition to full and productive employment and decent work for all. To achieve this in the next 10 years, target 8.1 aims to sustain per-capita economic growth worldwide “in accordance with national circumstances.” In particular, it makes the request for at least 7 percent gross domestic product growth to be achieved per annum in the least developed countries. This is a universal call for uninterrupted economic growth and prosperity from 2015 until 2030. Such growth will depend on technology, human-centered advancing manufacturing, and innovation. Recognizing this need, target 8.2 creates a benchmark to achieve higher levels of economic productivity through technological upgrading and innovation, including in high-value-added and labor-intensive sectors.

The financial system which underpins global economic activity—and which often precipitates economic downturns when vulnerable—is also at risk of cyberattacks. An Accenture study shows that over the next five years, banks stand to lose US\$347 billion, insurers US\$305 billion, and capital markets US\$47 billion from cybercrime.⁷³ Where cybercriminals are unrestricted and states do not prioritize working together to prosecute cybercrime based on universal principles, the financial institutions that manage global capital reserves are rendered vulnerable. Digital peace commitments are needed to mitigate the risk of financial system disruptions, which, in turn, pose unavoidable threats to the real economy and to the economic growth plan outlined in target 8.1.

In addition to the economic growth intentions, target 8.2 aims to achieve productive employment—“decent work for all.” This objective also faces real risks, stemming from cyber insecurity. The CSIS estimates that the US economy loses US\$100 billion from cybercrime and cyber espionage.⁷⁴ Notably, for “decent work,” it also indicated as many as 508,000 US jobs are lost annually as a result of malicious cyber activity.⁷⁵ Around the world, escalating cyber risks will further compound such job losses annually, with especially adverse effects in developing countries. Universal support for principles committing to digital peace in cyberspace sustains economic growth plans, secures financial nerve centers, and mitigates the risks of jobs losses from cyberattacks.

CASE IN POINT

As reported in the *Financial Times*, the head of Britain’s domestic Security Service MI5 announced in 2012 that state-sponsored cyberattacks against the computer systems of a major listed British company cost it £800 million in lost potential revenues, highlighting the huge threat that UK business faces from internet-based espionage. Jonathan Evans, MI5’s then-director general, said the amount of hostile activity being generated by foreign states in cyberspace was “astonishing.”

⁷³ Thompson, Chris. “What will cybercrime cost your financial firm?” Accenture, July 15, 2019. <https://www.accenture.com/us-en/insights/financial-services/cost-cybercrime-study-financial-services>

⁷⁴ Lewis, James Andrew. “CSIS Releases First Study to Connect Cybercrime to Job Loss,” CSIS, July 22, 2013. <https://www.csis.org/news/csis-releases-first-study-connect-cybercrime-job-loss>

⁷⁵ Ibid.

Digital Peace and SDG 9: Industry, Innovation and Infrastructure



This Sustainable Development Goal aims to build resilient infrastructure, promote inclusive and sustainable industrialization, and foster innovation. To achieve this in the next 10 years, target 9.1 calls for stakeholders to “develop quality, reliable, sustainable, and **resilient infrastructure**,” including regional and transborder infrastructure. The UN ECOSOC acknowledges that cyberattacks pose grave risks to industry and infrastructure.⁷⁶

The UN’s foremost economic and social organ further advised that “the economic impact and consequences of cyberattacks against critical physical infrastructure, the banking system, national health systems, essential government, and industry databanks and services could be extremely high.” The WannaCry and NotPetya cyberattacks in 2017, described earlier in this document, have unfortunately proven the ability of state-sponsored cyberattacks to cripple each of those industries, as warned by the UN ECOSOC, in dozens of countries—within an instant.

With respect to innovation, in its 2019 [Global Risks Report](#), the World Economic Forum warns that “Internet of Things have deepened connectivity across the world, increasing the potential for malicious actors to mount online attacks and amplifying their potential damage.”

Building resilience against such cyber risks with universal norms will help to secure the next generation of hyperconnected technology. At present, malicious actors in cyberspace already rely on the connectivity of digital citizens for their campaigns. In July 2020, a coordinated cyberattack took over the Twitter accounts of household names with large followings, including former US President Barack Obama, Democratic presidential nominee Joe Biden, the corporate accounts of Apple and Uber, and a host of US business leaders—from Bill Gates and Warren Buffet to Elon

Musk and Jeff Bezos.⁷⁷ The hackers posted apparent invitations encouraging their victims’ followers to send money into a “giving back” scheme that promised to return twice the amount, which served as a front for a Bitcoin scam.⁷⁸ All technology companies and related stakeholders need to build resilience to cyber risks online to protect people from malicious actors who misuse the technology and innovations that are woven into modern life. Taking

CASE IN POINT

As reported in *The Guardian*, a cyber weapon called the Mirai botnet shut down a significant portion of the internet in the United States in 2016, bringing down a number of sites, including Twitter, *The Guardian*, Netflix, Reddit, CNN, and many others in Europe. There are foreseeable risks that such cyber weapons could fall into the hands of state actors who could launch sophisticated cyber operations that effectively work against the intentions set out in goal 9.

⁷⁶ Statement by H.E. Mr. Lazarous Kapambwe, President of ECOSOC. “Special Event on Cybersecurity and Development,” December 9, 2011. https://www.un.org/en/ecosoc/president/statement_2011/statement_ecosoc_president_opening_remark-9_dec_2011.pdf

⁷⁷ Frier, Sarah, and Kartikay Mehrotra. “Twitter Hack Hits Obama, Biden, Musk in Bitcoin Scam,” Bloomberg, July 15, 2020. <https://www.bloomberg.com/news/articles/2020-07-15/elon-musk-bill-gates-appear-to-have-twitter-accounts-hacked>

⁷⁸ Ibid.

risk prevention measures also reduces the possibility of states launching such a model of cyberattacks, which abuse innovations and target household names, for geostrategic intentions.

The UN ECOSOC findings mentioned earlier expressly stated that “developing countries, with relatively weak surveillance capacity, are most vulnerable to cyberattacks.”⁷⁹ If these risks remain unmitigated, plans to upgrade infrastructure and to create global access to innovation and industry for all remain vulnerable to cyberattacks, which diminish collective trust in technology.

Recognizing the need for inclusivity, target 9.1 specifies a focus on “affordable and equitable access for all.” In other words, industry, innovation, and infrastructure must be inclusive and affordable to serve overall economic and human well-being. This is emphasized in target 9.5, which requires that stakeholders must upgrade the technological capabilities of industrial sectors in all countries—especially in developing countries.

In summary, the Fourth Industrial Revolution depends on trust in the safety of the technology it offers people, companies, and countries. Aligning on universal norms for digital peace in cyberspace will secure the digital foundations of the Fourth Industrial Revolution.

⁷⁹ Statement by H.E. Mr. Lazarous Kapambwe, President of ECOSOC. “Special Event on Cybersecurity and Development,” December 9, 2011. https://www.un.org/en/ecosoc/president/statement_2011/statement_ecosoc_president_opening_remark-9_dec_2011.pdf

Digital Peace and SDG 11: Sustainable Cities and Communities



This Sustainable Development Goal aims to make cities and human settlements inclusive, safe, resilient, and sustainable. To achieve this objective, target 11.b calls for stakeholders to increase the number of cities and human settlements adopting and implementing integrated policies to build resilience to disasters. The scope of disasters which warrant resilience-building includes cyber disasters, according to Mami

Mizutori, Assistant Secretary-General and Special Representative of the Secretary-General for Disaster Risk Reduction in the United Nations Office for Disaster Risk Reduction. Mizutori points out the Sendai Framework, the yardstick referenced in target 11.b, extends to hazards that are both natural to human-made.⁸⁰ Cyberattacks pose a human-made risk to safe cities and communities.

Target 11.2 highlights safe transportation systems as one of the backbones of infrastructure required for sustainable cities. Transportation systems of the future will require mitigation from cyber risks. According to the 2019 IBM X-Force Threat Intelligence Index, the transportation industry has become a priority target for cybercriminals.⁸¹ In 2018, it was the second-most attacked sector after the financial services sector.⁸² In 2019, simulations from ScienceDaily showed that mass cyberattacks on connected vehicles could send an entire city into gridlock.⁸³

Another cyber risk facing this goal lies in smart buildings. Digital technologies provide solutions for smart buildings to reduce the adverse per-capita environmental impact of cities, which is the objective set in target 11.6. Cyber risks threaten smart buildings, given their foreseen reliance on connected infrastructure and the Internet of Things (IoT),⁸⁴ as part of an effort to fit into sustainable city goals.

CASE IN POINT

According to *Forbes*, the independent Caribbean nation of Sint Maarten suffered a cyberattack in 2018 that shut down all government infrastructure for an entire day. Also, as reported in the *World Economic Forum*, from 2017–2018, in the United States alone, Atlanta, Baltimore, Charlotte, Dallas, and San Francisco all suffered cyberattacks. Such citywide cyberattacks constitute one element of the risks that undermine the goal of sustainable cities and communities.

⁸⁰ "Europe's concern over emerging risks," United Nations Office for Disaster Risk Reduction, November 18, 2018. <https://www.undrr.org/news/europes-concern-over-emerging-risks>

⁸¹ "IBM X-Force Report," February 26, 2019. <https://newsroom.ibm.com/2019-02-26-IBM-X-Force-Report-Ransomware-Doesnt-Pay-in-2018-as-Cybercriminals-Turn-to-Cryptojacking-for-Profit>

⁸² Ibid.

⁸³ "Hackers could use connected cars to gridlock whole cities," Science News and Georgia Institute of Technology, July 29, 2019. <https://www.sciencedaily.com/releases/2019/07/190729111337.htm>

⁸⁴ "How Digital Solutions Will Drive Progress Towards The Sustainable Development Goals," Accenture Strategy and Global e-Sustainability Initiative, 2016. http://systemtransformation-sdg.gesi.org/160608_GeSI_SystemTransformation.pdf

EY (formerly Ernst & Young) points out myriad risks that cyber insecurity poses to sustainable cities. For smart buildings, cyberattacks could disrupt digital alarm management systems and energy management.⁸⁵ Surveillance technology and insecure sensors are also prone to hacking, which would allow attackers to feed in fake data, cause signal failures, and effect shutdowns across cities.⁸⁶ Universal support for principles committing to digital peace in cyberspace secures the digital architecture, social structure, and economic promise of sustainable cities.

⁸⁵ "Cyber Security: A necessary pillar of Smart Cities," EY Report, 2016. <http://iranarze.ir/wp-content/uploads/2019/09/10116-English-IranArze.pdf>

⁸⁶ Ibid.

Digital Peace and SDG 16: Peace, Justice and Strong Institutions



This Sustainable Development Goal aims to promote peaceful and inclusive societies for sustainable development, provide access to justice for all, and build effective, accountable, and inclusive institutions at all levels. According to the CSIS, since 2006, state actors have staged cyberattacks, which target government institutions, media and journalists, courtrooms, diplomats, and elections,⁸⁷—among other stakeholders—in all corners of the world.

These risks pose an existential threat to a vital aspect of the social contract in democracies around the world. How will democracies be preserved if the legitimacy of our elected representatives can no longer be trusted? Cyberattacks have demonstrated their ability to disrupt electoral processes and, by extension, the peace and the integrity of institutions around the world. State-affiliated cyberattacks impacted the US presidential elections in 2016⁸⁸ and French presidential elections in 2017,⁸⁹ and they were responsible for a spate of election interferences in 2019 across Africa.⁹⁰ State-sponsored cyberattacks have led to shutdowns of private, media, and government institutions in Georgia in 2020.⁹¹ As these cyberattacks have proliferated and targeted civic institutions, some developing countries are now investing in cyber offensive capabilities,⁹² taking scarce investment capital away from competing development priorities. This step undermines the goal of sustainable development and peacebuilding. Universal digital peace commitments offer a tool for de-escalating the potential for cyber warfare and offer to help secure national institutions vital to peace.

Notably, election hackers particularly pose risks to target 16.7, which is to ensure responsive, inclusive, participatory, and representative decision-making at all levels. In summary, cyber risks threaten the integrity of elections all over the world. Mitigating this risk, principle three of the 2018 Paris Call for Trust and Security in Cyberspace,⁹³ commits stakeholders to strengthen their capacity—specifically to prevent malign interference by foreign actors to undermine electoral processes through malicious cyber activities.

CASE IN POINT

Bloomberg reported that Libya arrested two men in July 2019 who were accused of working for a Russian troll farm seeking to influence elections in the oil exporter and other African countries. The **Stanford Cyber Policy Center** lists Central African Republic, Democratic Republic of Congo, Libya, Madagascar, Mozambique, and Sudan as targets of a Russia-linked influence operation in Africa.

⁸⁷ "Significant Cyber Incidents," CSIS. <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>

⁸⁸ "Factbox: U.S. intel report on Russian cyberattacks in 2016 election," Reuters, January 26, 2017. <https://www.reuters.com/article/us-usa-russia-cyber-intel-factbox/factbox-u-s-intel-report-on-russian-cyber-attacks-in-2016-election-idUSKBN14Q2HH>

⁸⁹ Daniels, Laura. "How Russia hacked the French election," Politico, April 23, 2017. <https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/>

⁹⁰ In its 2019 report, the Stanford Cyber Policy Center lists Central African Republic, Democratic Republic of Congo, Libya, Madagascar, Mozambique, and Sudan as targets of a Russia-linked influence operation in Africa.

⁹¹ Ibid.

⁹² Reed, John. "Vietnam army reveals 10,000-strong cyber warfare unit," *Financial Times*, December 26, 2017. <https://www.ft.com/content/ef924a6e-ea14-11e7-bd17-521324c81e23>

⁹³ Find more details in the third section of this white paper.

Beyond institutions and elections, cyber risks also threaten individuals in societies embarking on digital transformation agendas. Recognizing the importance of population data for development, target 16.9 aims for states to provide legal identity for all by 2030. The [ID2020 Alliance](#) is a multistakeholder effort, building a new global model for the design, funding, and implementation of digital ID solutions and technologies. Working with the United Nations High Commissioner for Refugees (UNHCR), the alliance set a manifesto which considers the right to prove one's identity as a fundamental human right.⁹⁴ To deliver on target 16.9, efforts of this nature, which seek to deliver user-managed, privacy-protecting, and portable digital ID will require protection from cyberattacks that target personal data for malicious purposes. Without mitigating these cyber risks, trust in technology needed to deliver on human rights and identity solutions critical to sustainable development will be lacking among governments, societies, and people.

Digital peace in cyberspace based on global principles will offer modern societies and all peacebuilding government institutions significant digital protection.

⁹⁴ ID2020 Alliance Manifesto. <https://id2020.org/manifesto>

Digital Peace and SDG 17: Partnerships for the Goals



This Sustainable Development Goal works to strengthen the overall means of implementing the agenda and revitalizes global partnerships for sustainable development. In outlining the components of this goal, the UN classes technology as an essential means of implantation for achieving this goal. Specifically, target 17.6 calls for enhanced North-South, South-South, and triangular regional and international cooperation on access to science, technology, and innovation. In summary, target 17.6 aims to enhance the sharing of technology and innovation around the world to achieve the goals.

As stakeholders around the world embark on digital transformation, cyberattacks threaten a code-based digital world. Because the UN has affirmed technology is an essential means of implementation for the SDGs, the prevailing trust and safety concerns in the geopolitics of technology—on subjects ranging from 5G and the Internet of Things (IoT) to the ethics of artificial intelligence—threaten the call for global technology sharing to further development objectives. To mitigate the current geopolitical tensions, which effectively prevent technology sharing for development, stakeholders must commit to digital peace. Universal cybersecurity principles that ensure digital peace for our homes, our cities, and our social structures and infrastructure will build collective trust and safety in modern technology necessary for implementing sustainable development.

Cyberattacks have significantly evolved beyond the “first generation” cases of identity theft and email account hacks. A host of digital advancements, such as automated botnets and cloud computing architecture, can facilitate monumental cyberattacks—and defend against them. Universal digital peace commitments contribute to a world where stakeholders rally technological advancements

to protect people, businesses, and governments. As stakeholders design a sustainable future predicated on technology, they must also protect against an invisible enemy—cyberattacks—which could potentially cause shutdowns of the scale witnessed during the coronavirus pandemic and could risk sustainable development objectives.

CASE IN POINT

According to the [CSIS](#), in August 2019, a previously unidentified Chinese espionage group was found to have worked since 2012 to gather data from foreign firms in industries identified as strategic priorities by the Chinese government, including telecommunications, healthcare, semiconductor manufacturing, and machine learning. The group was also active in the theft of virtual currencies and the monitoring of dissidents in Hong Kong. These attacks affected various categories of technology. Goal 17 lists technology as one of the means of implementation necessary to deliver the SDGs.





Finally, target 17.8 aims to enhance the use of enabling technology for least developing countries in particular. A report published by the Centre on Cybersecurity at the Institute of International Political Studies predicts that with the development of the IoT, the cyber domain will connect more than 75 billion devices, many of which will control key functions of our daily lives and most of our critical infrastructure.⁹⁵ Accordingly, the ISPI report warns that the cyber domain has already become—and will increasingly be—the arena where national security and national interests naturally collide.





Digital peace in cyberspace based on principles with universal support will build trust in the technology needed to diffuse, deliver, and sustain the Sustainable Development Goals.




⁹⁵ Ruge, Fabio. "Confronting an 'Axis of Cyber'?" ISPI online, October 2018. https://www.ispionline.it/sites/default/files/pubblicazioni/cyber_def_web2.pdf

Shortlist of country positions on the policy link between cybersecurity and sustainable development

COUNTRY	STATEMENT
<p data-bbox="295 499 391 521">Australia</p> 	<p data-bbox="547 506 1406 678">"Australia's Cyber Cooperation Program (...) plays an important role in supporting Australia's international cyber engagement, which champions an open, free and secure cyberspace that protects national security and promotes international stability, while driving global economic growth and sustainable development. The Program supports Australia's commitment to deliver on the United Nations 2030 Agenda for Sustainable Development, which recognises the vital role of digital technologies to achieve a better and more sustainable future for all."</p> <p data-bbox="459 734 1382 786"><i>Source: Australian Paper – Open Ended Working Group on Developments in The Field of Information and Telecommunications in the Context of International Security (September 2019)</i></p>
<p data-bbox="300 835 386 857">Ecuador</p> 	<p data-bbox="547 891 1390 976">"Digital space should be preserved from militarization, and (...) concerns about the possible disruption of technical infrastructure essential to political processes such as elections, referenda or plebiscites should also be more widely reflected."</p> <p data-bbox="459 1077 1361 1155"><i>Source: Ecuador preliminary comments to the Chair's "Initial pre-draft" of the Report of the United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) (April 2020)</i></p>
<p data-bbox="256 1200 429 1223">European Union</p> 	<p data-bbox="547 1216 1382 1386">"The EU and its Member States are concerned by the rise of malicious behaviour in cyberspace by both state and non-state actors, including the abuse of Information and Communications Technologies (ICTs) for malicious purposes as well as cyber-enabled theft of intellectual property. Such behaviour undermines and threatens the integrity, security, economic growth and stability of the global community, and can lead to destabilising and cascading effects with enhanced risks of conflict."</p> <p data-bbox="459 1447 1297 1525"><i>Source: Joint comments from the EU and its Member States on the initial 'pre-draft' report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security</i></p>
<p data-bbox="292 1570 397 1592">Indonesia</p> 	<p data-bbox="547 1585 1398 1756">"...the advancement of new technologies such as Artificial Intelligence (AI), cloud computing and the Internet of Things (IoT). In this regard, we underline the that new technologies do not represent a threat to international peace and security by themselves, but rather their misuse and irresponsible behavior of state and non-state actors in using ICTs. Indonesia underlines the importance of widening of understanding, awareness and engagement, especially for regions and sub-regions that have yet to partake in cyber security discourse."</p> <p data-bbox="459 1816 1366 1868"><i>Source: Indonesia's Response on the Pre-Draft Report of the UN OEWG on the developments in the field of ICT in the context of international security</i></p>

COUNTRY	STATEMENT
<p data-bbox="300 371 384 398">Mexico</p> 	<p data-bbox="544 394 1393 539">"Mexico holds the strong conviction that only through multilateralism will the international community be able to assure, with a long-term vision the legitimate and peaceful uses of cyberspace, the resilience in the digital environment and the realization of the possibilities of information technologies to be used as enablers of sustainable development to leave no one behind."</p> <p data-bbox="456 600 1318 678"><i>Source: Preliminary comments of Mexico to the initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security</i></p>
<p data-bbox="272 723 411 750">New Zealand</p> 	<p data-bbox="544 739 1406 943">"Developments in ICTs have implications for all three pillars of the United Nations' work: peace and security, human rights and sustainable development. In parallel to the work on the topic of ICTs in the context of international security, discussions on other aspects of digital technologies have advanced in various UN bodies and agencies. These include matters related to digital cooperation, Internet governance, sustainable development, and human rights (including on data protection and privacy, freedom of expression, and freedom of information), as well as cybercrime and the use of the Internet for terrorist purposes."</p> <p data-bbox="456 1003 1377 1055"><i>Source: Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security</i></p>
<p data-bbox="300 1104 384 1131">Nigeria</p> 	<p data-bbox="544 1131 1334 1245">"There is a need to establish normative frameworks for responsible state behaviour in cyberspace (...) reliable attribution mechanisms will be needed and this requires the establishment of a neutral international cyber attribution agency. There is a need for cybersecurity capacity building in developing countries..."</p> <p data-bbox="456 1317 1370 1368"><i>Source: Statement at the meeting of the first substantive session of the Open-Ended Working Group (OEWG) (September 9, 2019)</i></p>
<p data-bbox="209 1417 480 1444">Non-Aligned Movement</p> 	<p data-bbox="544 1473 1406 1648">"NAM calls for the intensification of efforts towards safeguarding cyberspace from becoming an arena of conflict and ensuring instead the exclusive peaceful uses which would enable the full realization of the potential of ICTs for contributing to social and economic development. NAM reiterates its strong concern at the growing resort to unilateralism, and in this context, underlines that multilateralism and multilaterally agreed solutions, in accordance with the UN Charter, provide the only sustainable method of addressing international security issues."</p> <p data-bbox="456 1749 1374 1827"><i>Source: NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (OEWG)</i></p>

COUNTRY	STATEMENT
<p data-bbox="284 371 400 400">Singapore</p> 	<p data-bbox="544 378 1390 546">“Singapore underscores the importance of maintaining a technology-neutral approach when implementing measures to promote responsible State behaviour in cyberspace. It is the malicious use of technology, and not the technology itself that is a threat. Nevertheless, we agree that while technological advances and their new applications provide substantial benefits, they may also expand the attack surface and amplify vulnerabilities in the ICT environment.</p> <p data-bbox="544 577 1358 658">“More cooperation is necessary to protect and deal with threats to supranational critical information infrastructure (CII), which are owned by private companies, operate across national borders, and are not under any particular State’s jurisdiction.”</p>
<p data-bbox="456 703 1211 732"><i>Source: Singapore’s written comment on the Chair’s pre-draft of the OEWG report</i></p>	
<p data-bbox="276 770 411 799">South Africa</p> 	<p data-bbox="544 813 1390 927">“The growing exploitation or abuse of ICTs that hinders access to technologies and where access has established presents challenges to the full enjoyment of digital connectivity for economic and social development and the threats of insecurity of ICTs inhibits the ability of States to secure the gains already achieved.”</p>
<p data-bbox="456 1010 1406 1061"><i>Source: South Africa’s inputs and comments on the “Pre-draft” of the report of the OEWG on development in the Field of Information and Telecommunications in the context of International Security</i></p>	
<p data-bbox="300 1102 387 1131">Sweden</p> 	<p data-bbox="544 1126 1398 1267">“We believe that reduction or disruption of connectivity itself deserves attention as well. The ongoing tendencies towards regionalization and fragmentation of cyberspace ultimately threatens to harm global development. We stress the need for accepted principles, shared responsibilities and multi-stakeholder approaches. We support proposals to integrate the link between capacity building at the UN Sustainable Development Goals.”</p>
<p data-bbox="456 1330 1358 1382"><i>Source: Sweden’s comments on the Initial “Pre-draft” of the report of the UN Open Ended Working Group (April 15, 2020)</i></p>	
<p data-bbox="280 1420 406 1449">Switzerland</p> 	<p data-bbox="544 1440 1406 1615">“Switzerland agrees that the report of the (UN) OEWG be situated in the broader perspective and purpose of the United Nations. It has long been acknowledged that the three pillars of the UN—human rights, sustainable development and peace and security—are interdependent and mutually reinforcing. We believe that this ‘cross-pillar’ approach to the prevention of conflict and the maintenance of international peace and security could be brought out more strongly.”</p>
<p data-bbox="456 1668 1369 1749"><i>Source: UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, 2019/2020; written feedback by Switzerland to the first pre-draft report of the OEWG (April 9, 2020)</i></p>	

COUNTRY	STATEMENT
<p data-bbox="252 371 435 398">The Netherlands</p> 	<p data-bbox="544 378 1398 580">“Building cyber capacity proves essential in order to work towards achieving all 17 SDGs, and, as we argued in this paper, specifically goals 9 on resilient infrastructure, 10 on reducing inequality and 5 on gender equality. In order to improve and maintain a free, open and secure internet, it is essential to bridge the digital divide that exists between technologically developing and developed countries. Therefore, we encourage the (UN) GGE and OEWG to take consideration of the link between cyber capacity building and the achievement of the SDGs...”</p> <p data-bbox="456 627 1315 678"><i>Source: The Kingdom of the Netherlands non-paper: Cybersecurity Capacity Building and the Sustainable Development Goals</i></p>
<p data-bbox="296 719 392 745">Uruguay</p> 	<p data-bbox="544 779 1406 864">“The construction of an open, safe and reliable cyberspace cannot be a task only for governments. Participation in capacity building is important not only for state actors but also international organizations, civil society and the technical community.”</p> <p data-bbox="456 972 1078 999"><i>Source: Comments on the pre-draft of the OEWG report—Uruguay</i></p>
<p data-bbox="284 1043 400 1070">Zimbabwe</p> 	<p data-bbox="544 1055 1374 1223">“It is our shared concern that development of offensive ICT capabilities, militarisation of the cyberspace, cyber-attacks, cyber-crimes as well as cyber terrorism are now a global menace and significantly pose grave threats to the security and stability of nations. Global governance in cyberspace is a significant task for the international community. States should work together to create a multilateral, democratic and transparent global Internet governance system.”</p> <p data-bbox="456 1283 1321 1361"><i>Source: Considerations on the Initial Pre-Draft of the Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security</i></p>

III. Global initiatives to sustain digital peace

What are the current international initiatives and commitments working toward digital peace? Why should governments build on best practice policies and universally commit to principles for digital peace in cyberspace, including to protect the SDGs?

Developing commitments for digital peace

Commitments to digital peace can be structured and implemented in different ways to help stakeholders manage broadly applicable cybersecurity risks to the SDGs. Three approaches are important for policymakers to consider: UN processes, private sector approaches, and multistakeholder approaches. Although the source of protection differs in each case, all approaches are complementary and protect the necessary investments in the SDGs to a certain degree. The need to create a universal, government commitment to digital peace in cyberspace to comprehensively protect the SDGs is also considered.

United Nations (UN) working groups

The legal principles governing state behavior in cyberspace are still developing in international law. The United Nations General Assembly approved the creation of two groups to develop rules for responsible behavior in cyberspace.⁹⁶ First is the **United Nations Group of Governmental Experts (GGE)** on advancing responsible state behavior in cyberspace in the context of international security. Taking into account its previous iterations, six UN GGE working groups have been established since 2004, including the GGE 2019–2021. This UN GGE has been credited with introducing the principle that international law and, in particular, the United Nations Charter, is applicable and is essential to maintaining peace and stability and to promoting an open, secure, peaceful, and accessible ICT environment.⁹⁷ The current UN GGE 2019–2021 working group continues to study this issue while inviting national contributions on how international law applies to ICT. It's made up of 25 Member States,⁹⁸ with Brazil serving as the group chair.

Second is the **United Nations Open-Ended Working Group** on developments in the field of information and telecommunications in the context of international security (OEWG). Describing its intentions for setting up the OEWG, the UN affirmed its creation serves the purpose of "making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent (and) acting on a consensus basis, to continue, as a priority, to further develop the rules, norms, and principles of responsible behavior of States (and) the ways for their

⁹⁶ Barrinha, Andre. "The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace," *Council on Foreign Relations blog*, June 10, 2020. <https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace>

⁹⁷ "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, June 24, 2013. <https://undocs.org/A/68/98>

⁹⁸ Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States, Uruguay

implementation.”⁹⁹ UN OEWG is mandated to produce a consensus report to create common ground and mutual understanding among all Member States of the United Nations. It is open to all UN Member States, with Switzerland currently serving as the group chair.

In the UN GGE, participants have identified global risks that bear an impact on the SDGs. The existing and emerging threats they raise include misuse of social media and data, including during electoral processes, risks associated with the Internet of Things (IoT), and increasingly autonomous technology.¹⁰⁰ Threats identified in the misuse of social media during elections pose a direct risk to SDG 16.7 (Peace, Justice and Strong Institutions), which aims to ensure responsive, inclusive, participatory, and representative decision-making at all levels. The UN OEWG participants have identified threats to critical infrastructure, including the public core of the internet as a concern.¹⁰¹ Entities that owned or controlled critical infrastructure were shown to be at particular risk.¹⁰² Members also singled out the financial sector as often the target of cyber operations. This threat poses a direct risk to target 1.4 (No Poverty), which aims to ensure that all men and women—in particular the poor and the vulnerable—have equal rights to economic resources to appropriate new technology and financial services. Despite ongoing efforts of both the UN GGE and UN OEWG, there remains a need for an alignment on global norms and principles, which responds to the cyber risks that both groups have identified as threatening the attainment of mission-critical SDGs—including poverty, peace, and partnerships in technology.

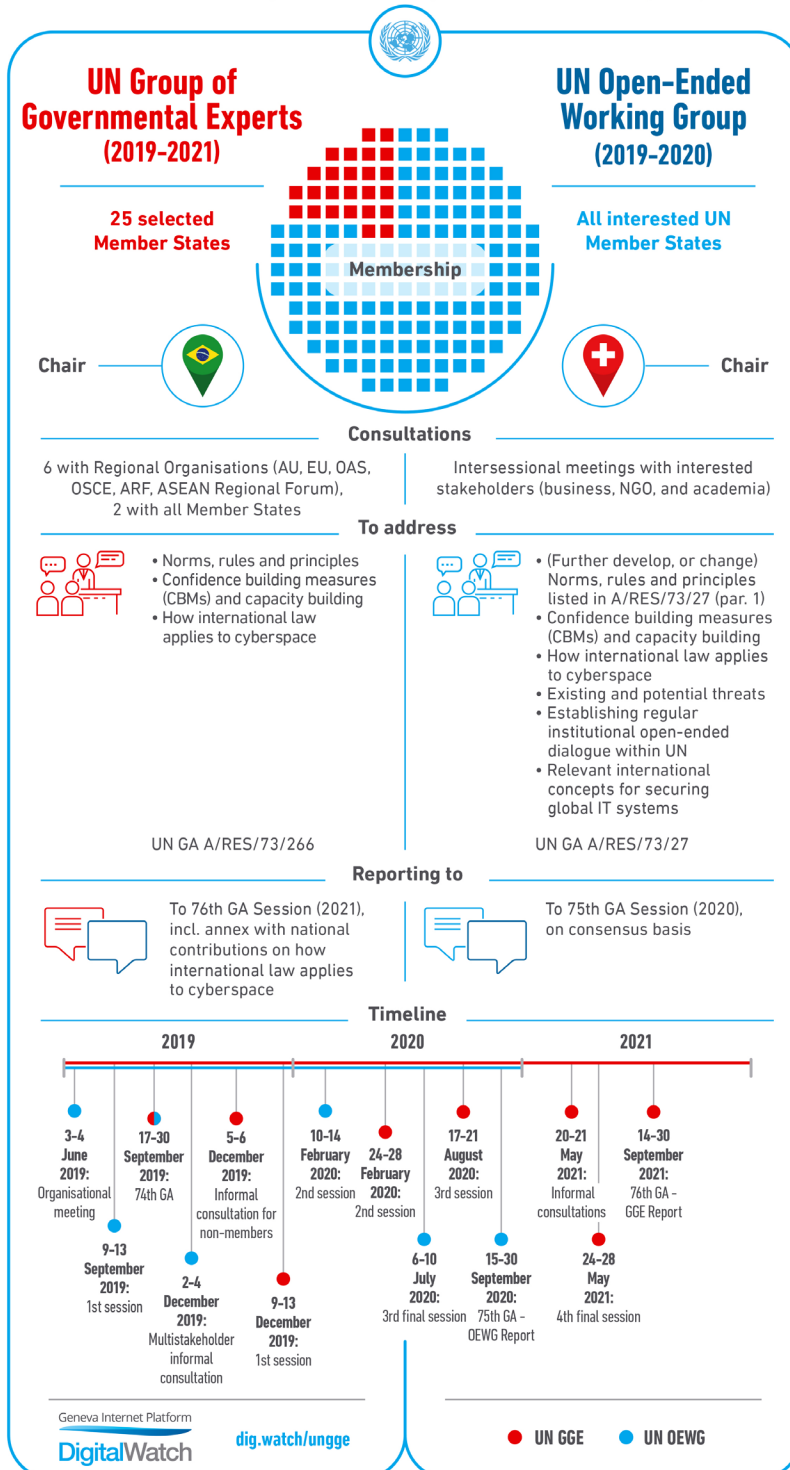
⁹⁹ “Developments in the field of information and telecommunications in the context of international security,” United Nations General Assembly, December 11, 2018. <https://undocs.org/A/RES/73/27>

¹⁰⁰ UN GGE Chair’s Summary, December 2019. <https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf>

¹⁰¹ UN OEWG Chair’s letter, January 28, 2020: paragraph 11. <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/200128-OEWG-Chairs-letter-on-the-summary-report-of-the-informal-intersessional-consultative-meeting-from-2-4-December-2019.pdf>

¹⁰² UN OEWG Chair’s letter, January 28, 2020. <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/200128-OEWG-Chairs-letter-on-the-summary-report-of-the-informal-intersessional-consultative-meeting-from-2-4-December-2019.pdf>

Comparative Survey of the two UN-based processes on responsible behaviour in cyberspace



United Nations policy frameworks

Global Commitment on Digital Trust and Security

In July 2018, the United Nations Secretary-General convened the [High-level Panel on Digital Cooperation](#) to provide recommendations on how the international community could work together to optimize the use of digital technologies and to mitigate the risks. In June 2019, the panel published its report, “[The Age of Digital Interdependence](#),” with a series of recommendations to improve digital cooperation.

One of the report’s recommendations is the development of a Global Commitment on Digital Trust and Security. The recommendation is a call to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action. The “Age of Digital Interdependence” report articulates the commitment in the following terms:

As the digital economy increasingly merges with the physical world and deploys autonomous intelligent systems, it depends ever more on trust and the stability of the digital environment. Trust is built through agreed standards, shared values and best practices. Stability implies a digital environment that is peaceful, secure, open and cooperative. More effective action is needed to prevent trust and stability being eroded by the proliferation of irresponsible use of cyber capabilities.

The Global Commitment on Digital Trust and Security could build on and create momentum behind the voluntary norms agreed in the report of the 2015 GGE, and complement relevant global processes.

It could address areas such as ways to strengthen implementation of agreed norms; developing societal capacity for cybersecurity and resilience against misinformation; encouraging companies to strengthen authentication practices, adhere to stricter software development norms and be more transparent in the use of software and components; and improving the digital hygiene of new users coming online.

The panel further recommends that the UN Secretary-General facilitates an agile and open consultation process to develop updated mechanisms for global digital cooperation. Proclaiming the urgent need for a consultation process, the panel suggested marking the UN’s 75th anniversary in 2020 with a “Global Commitment for Digital Cooperation” to enshrine shared values, principles, understandings, and objectives for an improved global digital cooperation architecture. As part of this process, the panel noted that the UN Secretary-General may appoint a Technology Envoy.

The United Nations Secretary-General’s Roadmap on Digital Cooperation

In June 2020, the United Nations Secretary-General launched the [Roadmap for Digital Cooperation](#). The roadmap is based on recommendations from the Secretary-General’s High-level Panel on Digital Cooperation convened from 2018–2019, chaired by Melinda Gates and Jack Ma, and further informed by a series of roundtable discussions with key stakeholders from government, the private sector, civil society, international organizations, academic institutions, the technical community, and [other relevant stakeholders](#).

The roadmap sets out eight key areas for action:

1. Achieving universal connectivity by 2030. Half of the world's population currently does not have access to the internet. By 2030, every person should have safe and affordable access to the internet, including meaningful use of digitally enabled services in line with the Sustainable Development Goals.
2. Promoting digital public goods to create a more equitable world. We must undertake a concerted global effort to encourage and invest in the creation of digital public goods: open-source software, open data, open AI models, open standards, and open content. These digital public goods should adhere to privacy and other applicable laws and best practices, do no harm, and help attain the SDGs.
3. Ensuring digital inclusion for all, including the most vulnerable. Digital divides reflect and amplify existing social, cultural, and economic inequalities. The gender gap in global internet use is a stark example—in two out of every three countries, more men use the internet than women. Similar challenges affect migrants, refugees, internally displaced persons, older persons, young people, children, persons with disabilities, rural populations, and indigenous peoples. We must close these gaps through better metrics, data collection, and coordination of initiatives.
4. Strengthening digital capacity-building. Many countries and citizens are deprived of capacities and skills crucial to the digital era and to attaining the SDGs. Digital capacity-building must be more needs-driven and tailored to individual and national circumstances and should be better coordinated globally.
5. Ensuring the protection of human rights in the digital era. Digital technologies provide new means to exercise human rights, but they are too often used to violate human rights. Regulatory frameworks and legislation on the development and use of digital technologies should have human rights at their center. Data protection, digital ID, the use of surveillance technologies, online harassment, and content governance are of particular concern.
6. Supporting global cooperation on artificial intelligence. AI brings enormous benefits to the digital era, but it can also significantly compromise the safety and agency of users worldwide. Enhanced multistakeholder efforts on global AI cooperation are needed to help build global capacity for the development and use of AI in a manner that is trustworthy, human rights-based, safe, and sustainable and that promotes peace.
7. Promoting trust and security in the digital environment. The digital technologies that underpin core societal functions and infrastructure, including supporting access to food, water, housing, energy, healthcare, and transportation, need to be safeguarded. A broad and overarching statement outlining common elements of an understanding on digital trust and security, endorsed by all Member States, could help to shape a shared vision for digital cooperation based on global values.
8. Building a more effective architecture for digital cooperation. There are significant gaps in global digital cooperation, and digital technology issues are too often low on political agendas. Even where there has been cooperation, it's frequently fragmented and lacks tangible outcomes or sound follow-up processes. As a starting point, the Internet Governance Forum must be strengthened to make it more responsive and relevant to current digital issues.

Private-sector approaches

The Cybersecurity Tech Accord

In April 2018, 34 private companies signed the [Cybersecurity Tech Accord](#), roughly one year after the WannaCry and NotPetya cyberattacks. The signatories commit to a mission of promoting a safer online world, specifically by fostering collaboration among global technology companies committed to protecting their customers and users and to helping them defend against malicious threats. Since then, the accord has garnered over 100 signatories who partner on initiatives that improve the security, stability, and resilience of cyberspace.

The accord sets out four private-sector commitments for collective action:

1. Provide their customers, users, and the developer ecosystem with information and tools that enable them to understand current and future threats and to better protect themselves.
2. Protect their customers and users everywhere by designing, developing, and delivering products and services that prioritize security, privacy, integrity, and reliability and, in turn, reduce the likelihood, frequency, exploitability, and severity of vulnerabilities.
3. Work with each other and like-minded groups to enhance cybersecurity best practices, such as improving technical collaboration, coordinated vulnerability disclosure, and threat-sharing, in addition to ensuring flexible responses for the wider global technology ecosystem.
4. Oppose efforts to attack citizens and enterprises by protecting against exploitation of technology products and services during their development, design, distribution, and use.

Siemens Charter of Trust

In February 2018, at the Munich Security Conference, Siemens and eight industry partners signed a joint charter for greater cybersecurity. Initiated by Siemens, the [Charter of Trust](#) calls for binding rules and standards to build trust in cybersecurity and to further advance digitalization. Since 2018, the Charter of Trust has grown to 16 members. In addition to Siemens and the Munich Security Conference, signatories include AES, Airbus, Allianz, Atos, Cisco, Daimler, Dell Technologies, Deutsche Telekom, IBM, NXP, SGS, Total, and TÜV Süd.

The charter sets out 10 principles for partners:

1. Ownership for cyber and IT security
2. Responsibility throughout the digital supply chain
3. Security by default
4. User-centricity
5. Innovation and co-creation
6. Education
7. Certification for critical infrastructure and solutions
8. Transparency and response
9. Regulatory framework
10. Joint initiatives

Multistakeholder approaches

The Paris Call for Trust and Security in Cyberspace

In November 2018, at the Internet Governance Forum (IGF), French President Emmanuel Macron launched the [Paris Call for Trust and Security in Cyberspace](#), a multistakeholder initiative led by the French government. The Paris Call focuses on nine fundamental principles to promote a safe and secure cyberspace for all. It has since garnered support across the globe—including more than 78 governments, 642 private-sector entities, and 347 civil society organizations—making it the largest cybersecurity-focused, multistakeholder commitment in the world.

The Paris Call commits stakeholders to work collaboratively on nine principles:

1. Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate, or systemic harm to individuals and critical infrastructure.
2. Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the internet.
3. Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.
4. Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or the commercial sector.
5. Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm.
6. Strengthen the security of digital processes, products, and services, throughout their lifecycle and supply chain.
7. Support efforts to strengthen an advanced cyber hygiene for all actors.
8. Take steps to prevent non-state actors, including the private sector, from hacking back, for their own purposes or those of other non-state actors.
9. Promote the widespread acceptance and implementation of international norms of responsible behavior, as well as confidence-building measures in cyberspace.¹⁰³

How does the Paris Call support the SDGs?

The Paris Call is the primary international cybersecurity commitment calling for stakeholders to protect “individuals and critical infrastructure.” In this respect, the **Paris Call principle one** offers the most digital protection for people, financial investments, and assets at the core of the SDGs agenda—through 2030 and beyond. For example, in **target 9.c** (Industry, Innovation and Infrastructure), the United Nations calls for universal and affordable access to the internet in the least developed countries. The **Paris Call principle two** ensures that the internet, including its continued expansion, remains a safe space. Internet protection also builds needed trust in the cyber integrity of 5G technology, which is of particular importance in 2020 and beyond.

¹⁰³ “Paris Call for Trust and Security in Cyberspace,” November 12, 2018. https://onu.delegfrance.org/IMG/pdf/paris_call_for_trust_and_security_in_cyberspace.pdf

Similarly, by seeking to protect electoral processes around the world from cyber risks, **principle three of the Paris Call** protects the goals for peace, justice, and institutions (SDG 16) in a climate where civic and democratic engagement is taking a digital dimension around the world.

Another example is shown in **target 9.5**, in which members states agreed to enhance scientific research, upgrade the technological capabilities of industrial sectors in all countries by 2030, in particular developing countries, including encouraging innovation. This target faces heightened risks from growing cyber theft, which undermines innovation and technological advancement. To support the innovation, **Paris Call principle four** commits to preventing ICT-enabled theft of intellectual property.

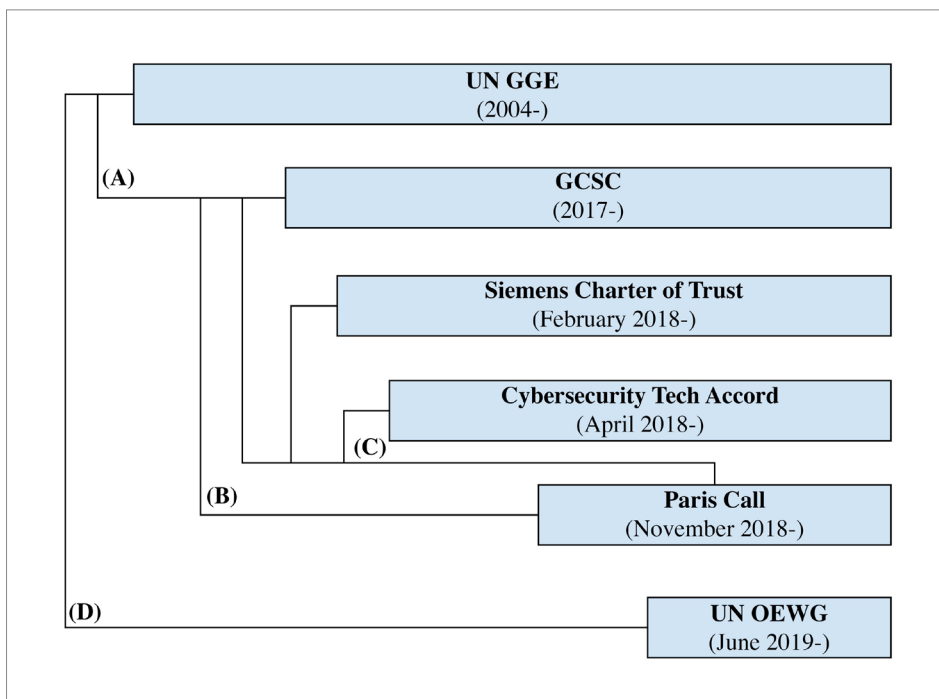
Additionally, in **target 9.c** the United Nations intends for a significant increase in access to information and communications technology universally. To ensure the increasing uptake in technology remains secure and safe, **principle five of the Paris Call** combats the proliferation of malicious ICT tools and practices around the world.

In many respects, the Paris Call commits stakeholders to protect mission-critical objectives in the SDGs. Target 9.a calls for Member States to facilitate sustainable and resilient infrastructure development in developing countries, including through “enhanced financial, technological and technical support to African countries.” To be sustainable, such rapid scaling of technology around the world rests on universal support for principles committing to digital peace in cyberspace, particularly in regions that are highly vulnerable to cyberattacks due to technical capacity limitations, along with the corresponding implications of cyber disruptions to the real economy.

The Global Commission on the Stability of Cyberspace

Established in February 2017, the **Global Commission on the Stability of Cyberspace** (GCSC) is a multinational body of experts drawn from government, academia, civil society, and the private sector. It has similarly released eight norms and a set of recommendations for advancing cyber stability, including protection for technical infrastructure essential to elections. Notably, its principles reflect the view that cyber stability is a responsibility for both state and non-state actors. The principles include responsibility—everyone is responsible for ensuring the stability of cyberspace. Second, it also calls for restraint—no state or non-state actor should take actions that impair the stability of cyberspace. Its third principle is a requirement to act—state or non-state actors should take reasonable and appropriate steps to ensure the stability of cyberspace. Finally, it includes a principle on the respect for human rights, which affirms that efforts to ensure the stability of cyberspace must respect human rights and the rule of law.

The Global Commission’s guidelines offer protection for cyber risks coming from non-state actors, which could also severely impact SDG infrastructure. Given that cyberattacks come from organized criminal groups, too, including terrorist organizations, the SDG infrastructure also needs cyber resilience to cyber terrorism. To protect the water, energy, transportation, and other critical infrastructure in the SDGs from cyber terrorism, states must cooperate on cyber stability risks. The commission recommendation in this respect includes state cooperation to exchange information and to assist in prosecution of terrorist and criminal use of ICT.



Source: Carnegie Endowment for International Peace

Why should governments universally commit to principles for digital peace in cyberspace?

Currently, the lack of leadership on digital peace from mission-critical states has led to a fragmented landscape of cyber norms governing state behavior.¹⁰⁴ Geopolitical divides in cybersecurity policy also prevent any one digital peace commitment from being adopted by all the key cyber actors on the world stage. The protection of “critical infrastructure” in cyberspace has experienced a mixed bag of successes and failures in global policy forums.¹⁰⁵ Crucially, even where this is alignment on the protection for critical infrastructure in cyberspace, this protection does not enjoy a corresponding universal alignment on the definition of critical infrastructure.¹⁰⁶

¹⁰⁴ Ruhl, Christian, et al. “Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads,” Carnegie Endowment for International Peace, February 26, 2020. <https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110>

¹⁰⁵ Nye, Joseph S. “Normative Restraints on Cyber Conflict,” Belfer Center for Science and International Affairs, August 2018. <https://www.belfercenter.org/sites/default/files/files/publication/Nye%20Normative%20Restraints%20Final.pdf>

¹⁰⁶ “Protection of ‘Critical Infrastructure’ and the Role of Investment Policies Relating to National Security,” OECD, May 2008. <https://www.oecd.org/daf/inv/investment-policy/40700392.pdf>

States have a responsibility to protect people and, by extension, the critical infrastructure that people depend on for economic and social well-being. To create the most robust protection from cyber risks, all states must build on existing initiatives with a detailed commitment to digital peace that protects the social structures and infrastructure covered in the SDGs—including digital education systems, healthcare systems, electricity systems, and sustainable cities. Committing to protect these parts of our world will provide resilience around the SDGs, while ensuring financial investments into the agenda are safeguarded through 2030 and beyond.

Alternatively, ambiguity around safe zones will be consistently exploited by malicious actors who use cyberattacks as a relatively inexpensive tool of statecraft. Once more, it's worth remembering that in March 2020 alone—amid global response efforts to the coronavirus pandemic—hospitals, medical facilities, government health agencies, and testing centers—and even the World Health Organization—faced targeted cyberattacks perpetrated by malicious actors.¹⁰⁷ Although various states have made crossing accusations related to the attribution of these cyberattacks, reports have linked four countries to the cyber offensive actions that undermine the fight against the coronavirus, spread disinformation, and work to gain access to US and WHO servers.^{108, 109}

The Geneva-based CyberPeace Institute (CPI) recognized the need to protect infrastructure in the healthcare sector from cyberattacks, including targeted incidents that exploit vulnerabilities amid a pandemic. In June 2020, CPI launched [Cyber 4 Healthcare](#), a healthcare-cybersecurity match-making service. Cyber 4 Healthcare aims to strengthen the cybersecurity of the healthcare sector, as it takes unprecedented measures to cope with the pandemic, while facing threats from malicious actors perpetrating new cyberattacks, targeting hospitals and healthcare organizations, and putting thousands of human lives at risk. Cyber 4 Healthcare connects healthcare organizations in need of cybersecurity advice with reputable actors willing to offer a wide range of cybersecurity assistance services—free of charge. The CyberPeace Institute is working with partners on the initiative, including Microsoft, Global Cyber Alliance, and Unisys, among others.

Taken together, such efforts work to build resilience around SDG 3 (Good Health and Well-Being) and to protect all stakeholder investments made to achieve the goal. This is one example. All classes of infrastructure in the SDGs stand to benefit from states committing to principles and norms that ensures digital peace in cyberspace.

¹⁰⁷ Ruhl, Christian. "Note to Nations: Stop Hacking Hospitals," Foreign Policy, April 6, 2020. <https://foreignpolicy.com/2020/04/06/coronavirus-cyberattack-stop-hacking-hospitals-cyber-norms/>

¹⁰⁸ Ibid.

¹⁰⁹ Menn, Joseph, et al. "Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus – sources," Reuters, April 2, 2020. <https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC>

The ICRC recently affirmed the universal protections of civilians and civilian infrastructure to exist in times of armed conflict.¹¹⁰ Paradoxically, these same protections do not yet exist in peacetime. Governments need to work to implement norms for nation state behavior that protect civilians, both in war and peace.

Table 1. National Definitions of Critical Infrastructure

Australia	“Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia’s ability to conduct national defence and ensure national security.”
Canada	“Canada’s critical infrastructure consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada.”
Germany	“Critical infrastructures are organisations and facilities of major importance to the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences.”
Netherlands	“Critical infrastructure refers to products, services and the accompanying processes that, in the event of disruption or failure, could cause major social disturbance. This could be in the form of tremendous casualties and severe economic damage...”
United Kingdom	“The [Critical National Infrastructure] comprises those assets, services and systems that support the economic, political and social life of the UK whose importance is such that loss could: 1) cause large-scale loss of life; 2) have a serious impact on the national economy; 3) have other grave social consequences for the community; or 3) be of immediate concern to the national government.”
United States	The general definition of critical infrastructure in the overall US critical infrastructure plan is: “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” For investment policy purposes, this definition is narrower: “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security.”

Source: “OECD Protection of ‘Critical Infrastructure’ and the Role of Investment Policies Relating to National Security,” 2018.

¹¹⁰ Menn, Joseph, et al. “Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus – sources,” Reuters, April 2, 2020. <https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC>; and articles 48, 51, and 52 “Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (API),” Rules 1 and 7 ICRC Customary IHL Study.

Conclusion

In a digital world, achieving the sustainable development agenda will depend on an invisible pillar of support—digital peace in cyberspace. A universal commitment to principles that secure the digital world offers more protection than a seatbelt or an airbag around the SDGs. It's a factor crucial to the success of the digital economy. People, governments, and organizations need to trust that digital technologies are secure, or they won't embrace the digital transformation. Around the world, more than 60 states already have—or are developing—cyber offensive capabilities. Although dozens of countries are committing to cybersecurity principles that reference the protection of critical infrastructure, a universal commitment to principles for digital peace in cyberspace affords the social structures and infrastructure at the heart of the SDGs the security needed in the modern era.

How governments approach this effort will profoundly affect global security, societal opportunity, and economic development—pillars of the Sustainable Development Goals. An approach that mitigates risks to the SDGs will provide assurances for stakeholders investing in the agenda—namely, a detailed commitment to digital peace that protects social structures and infrastructure covered in the SDGs is paramount. As a complement, prioritizing, tackling, and preventing all cybercrime in criminal justice systems around the world will help to address the specific challenge of nation-states exploiting cybercriminals. This calls for national capacity building for cyber policy and cyber practices. The results for governments—and for their partners in the private sector and beyond—will be improved cybersecurity, along with continued societal opportunity and economic growth.

