A Rules-Based Order to Keep the Internet Open and Secure

Marietje Schaake

When J. P. Barlow presented his 1996 "Declaration of the Independence of Cyberspace" in Davos, cyberspace was idealized as a separate universe, detached from the "real" world, with no government controls and no national boundaries.[1] Twenty-two years later, this libertarian dream of the open Internet has been buried with J. P. Barlow. The Internet has increasingly become an essential element to furthering people's development and freedom, as well as a foundation for economic growth and international trade. The stakes for nation-states to exercise control over its functioning have thus become higher, and the global Internet has now become a platform for political, economic, and military power. Additionally, private companies have become powerful global actors in the online environment.

The European Union and the United States have historically been the guardians and advocates of a rules-based system, and should be best positioned to develop global rules for the open Internet, based on the rule of law. However, there is a wide gap to be bridged between promise and practice. Both American and European leaders have had moments of promoting an open, free, and secure Internet as part of foreign policy. In 2010, US Secretary of State Hillary Clinton launched her Internet Freedom Strategy that promoted the freedom to connect, centered on "the idea that governments should not prevent people from connecting to the Internet, to websites, or to each other."[2] She urged media companies to "take a proactive role in challenging foreign governments' demands for censorship and surveillance."[3] The EU followed suit and promoted its No Disconnect strategy in the wake of the Arab Spring, which aimed to ensure that "information and communication technology can remain a driver of political freedom, democratic development and economic growth."[4] The High Representative of the European Union for Foreign Affairs and Security Policy, Catherine Ashton, stated that "the EU is determined to resist any unjustified restrictions on the Internet and other new media."[5]

However, the legacy of these much-touted

When J. P. Barlow presented his 1996 "Declaration of the Independence of Cyberspace" in Davos, cyberspace was idealized as a separate universe, detached from the "real" world, with no government controls and no national boundaries. Twenty-two years later, this libertarian dream of the open Internet has been buried with J. P. Barlow.

Marietje Schaake is a Dutch politician and Member of the European Parliament (MEP) from the Netherlands. She is a member of Democrats 66, part of the Alliance of Liberals and Democrats for Europe Party. *The Wall Street Journal* has called her "Europe's most wired politician," while CNN called her a "rising Dutch star" who makes an increasingly rare "passionate and public case for liberalism and globalization." She was voted as one of the "40 MEPs that matter" by *Politico* in 2016 and was selected as one of the "*Politico* 28" in 2017. According to *Politico*, Schaake is the "ultimate digital MEP."

The European Union and the United States have historically been the guardians and advocates of a rules-based system, and should be best positioned to develop global rules for the open Internet, based on the rule of law. However, there is a wide gap to be bridged between promise and practice.

"21st century statecraft"[6] policies is minimal. The EU has quietly abandoned its No Disconnect strategy,[7] and after the Snowden revelations, the US lost its credibility when it came to promoting online freedom. Similarly, in the wake of a number of terrorist attacks on European soil, the EU has proposed measures that have eroded the high standards on Internet freedom Europe had earlier promised to uphold.[8] In general, Europe focuses now almost exclusively on the potential threats that were associated with the rise of the Internet and new technologies, as opposed to focusing predominantly on its liberating effect. Both European and American companies continue at the same speed to export highly sophisticated surveillance systems to dictatorships.[9] Both actors have lost precious time to seek effective leadership toward a rules-based system to preserve the open Internet globally.

An alternative model to a global, rules-based online order is gaining ground in the meantime. China is a staunch defender of the idea that states should be permitted to manage and contain their "own Internet." A recent implementation of the concept of this "cyber sovereignty" is China's cybersecurity law, which requires foreign firms to store data on Chinese territory. These data can be transferred abroad only after "security assessments" that severely disrupt the free flow of information.[10] Other articles of the law disproportionately interfere with the right to privacy and the freedom of speech.[11] China actively seeks to shape global norms based on what it considers to be responsible state behavior online.[12] This model certainly does not put the rule of law, or the rights and freedoms of users, first. It also has a profoundly protectionist impact.

Governments exercising national control over the Internet also hurt cybersecurity. Nation-states are increasingly exploiting weak elements in the security architecture of the Internet to attack others. Intelligence services are stockpiling vulnerabilities in software, with the aim of weaponizing them or using them for covert access to devices and systems.[13] Almost two hundred state-sponsored attacks by sixteen countries have been registered since 2005, including twenty in 2016.[14] So it came as no surprise when NATO members recognized cyberspace as a fifth domain of operations "in which NATO must defend itself as effectively as it does in the air, on land, and at sea."[15] New dimensions of this fifth domain of warfare are manifesting themselves in a number of hybrid conflicts. The United States charged thirteen Russian nationals and three Russian firms for meddling in the presidential election of 2016. The indictment says that a Russian organization called the Internet Research Agency sought to wage "information warfare" to "sow discord" in the American political system with the use of fictitious personas, social media platforms, and other Internet-based media.[16]

Now even the initial taboo on states' sponsoring cyber-attacks that could result

Almost two hundred state-sponsored attacks by sixteen countries have been registered since 2005, including twenty in 2016.

in human casualties is crumbling. The *New York Times* has described a cyber-attack on a petrochemical plant in Saudi Arabia that not only meant to sabotage operations but also cause "an explosion that would have killed people."[17] In its annual report, the cybersecurity firm CrowdStrike warns against the boomerang effect of stockpiling security vulnerabilities. It suggests that in the future it will not just be nation-states that wield the most damaging hacking tools: "The result of trickle-down in the field of cybersecurity has been a proliferation of highly sophisticated weaponry for cyber warfare being pushed down into the mass market and commoditized."[18] The growing influence of the private sector has barely been dealt with in regulatory frameworks, even though the dependence of governments on companies to provide for critical infrastructure, as well as its protection, has changed the relationship between the public and private sectors significantly. As Professor Joseph Nye of Harvard University pointed out earlier, "Most of the Internet and its infrastructure belong to the private sector, and the government has only modest levers to use."[19]

The European Union is in the process of adopting laws that will make it more difficult for companies to sell ready-made surveillance systems to buyers with known human-rights violations. This is a rare example of regulation aiming to improve both cybersecurity and human rights.[20] Generally, the ambition to prevent hybrid conflicts from growing and escalating should be stepped up. To prevent, attribute, and attach consequences to attacks, a rules-based system needs to be further developed. Rules should also clarify the relationship between governments and the private sector when it comes to establishing responsibilities and obligations to protect citizens and objects that are connected to the Internet. While the state bears formal responsibility to protect citizens and to ensure national security, companies are less accountable.

Generally, the ambition to prevent hybrid conflicts from growing and escalating should be stepped up. To prevent, attribute, and attach consequences to attacks, a rules-based system needs to be further developed.

Increasingly, the private sector itself steps into the void of norms with the aim of securing and stabilizing cyberspace. Most recently, thirty-four tech companies put forward principles to "protect and empower civilians online and to improve the security, stability, and resilience of cyberspace" in the Global Cybersecurity Tech Accord.[21] While industry collaboration can contribute to stronger security standards, it can never replace the creation of responsible norms for state behavior in cyberspace and laws. Clearly, while private companies have a significant responsibility toward the public, they do not necessarily serve the public interest, and sometimes profit models and incentives are at odds with accountability and transparency. When a company finds a vulnerability in its software, will it choose to warn users and invest in patching the software or rather manage its reputation?

One would expect cybersecurity to be at the forefront of political agendas of the heads of state or ministers of defense who assembled at the annual Munich Security Conference in February 2018. But instead of looking for concrete ways to collectively address this complicated threat landscape, cybersecurity was not a top priority. Digital topics were featured prominently in side meetings, while the main stage was reserved for traditional foreign policy and defense topics. "It is tempting to think of

cyberspace as hovering over the real world and not actually connected to it," said one of the Internet's founders, Vint Cerf.[22] "But we create this virtual world through companies, facilities and users located in physical space." According to NATO assistant secretary general Sorin Ducaru, in geopolitical circles "cyber is still seen as a technical problem constricted to the virtual world."[23] This does not reflect the strategic importance of considering the integrated nature of digitization and connectivity in so many parts of society. Normative restraints on state behavior in cyberspace are needed in order to secure trust in digital infrastructure, protect human rights, and avoid a digital arms race.

United Nations secretary general António Guterres stated in Munich that it is "high time to have a serious discussion about the international legal framework in which cyberwars take place," and that it is "essential to use what is the competence of the First Committee of the General Assembly of the United Nations to do it, and to do it sooner rather than later."[24] While this is a laudable goal, the failure of the United Nations Group of Governmental Experts (UN GGE) in 2017 to reach a concluding document after thirteen years of relatively constructive discussion between states about restricting cyber warfare[25] does not bode well for the immediate future of the First Committee as a venue for discussing these issues. The challenge of reaching global agreement is a reminder of the different interests and visions of governments. These divisions are likely to get deeper, while the mutual dependence between states, companies, and citizens online still suggests agreements beyond national borders are needed.

Wolfgang Kleinwachter, a professor at the University of Aarhaus, has suggested an alternative framework to address cybersecurity issues with a more holistic approach combining security, economic, and social aspects. Such a broad scope could cover cybersecurity laws increasingly being used as protectionist measures to disrupt international trade, but the removal of content, justified with national security arguments, is also on the rise. Kleinwachter has compared the current "poly crises" with the situation in the 1960s, when the world was confronted with a multitude of crises (Cuba, the Six Day War, Vietnam, the nuclear arms race). He highlights that in the past a countermovement also emerged, culminating in the Conference on Security and Cooperation in Europe, to reduce tension:

> In the CSCE Final Act of 1975, the entire spectrum of conflict between East-West relations—from security to economic cooperation and human rights—was channeled into a coexistence that was not friction-free but well regulated. The ideological opponents did not give up their values. But the common interests in a peaceful and prosperous Europe had priority. Basically, cyberspace today deals with the same three CSCE topics: avoiding a cyber-war, shaping the digital economy and ensuring digital rights.[26]

This focus on common interests is a good starting point to scope out areas for common ground.

A modern-day "Helsinki process" could deal with issues that do not fall within the

The failure of the United Nations Group of Governmental Experts (UN GGE) in 2017 to reach a concluding document after thirteen years of relatively constructive discussion between states about restricting cyber warfare, does not bode well for the immediate future of the First Committee as a venue for discussing these issues.

UN GGE's ambit but that still have an impact on cybersecurity norms, including safety standards, the product liability issues of Internet infrastructure, content management, and the digital economy. Such a framework could be one way to come to reach global agreement on a norm to protect the core of the Internet, for example. The functioning of the core protocols of the global Internet is in the interest of governments, companies, and citizens worldwide. Professor Nye remarks, "Unlike the single strand of military interdependence that linked the United States and the Soviet Union during the Cold War, the United States, China, and other countries are entangled in multiple networks. China, for example, would itself lose from an attack that severely damaged the American economy, and vice versa."[27]

The incentives to find common ground will likely not be inspired by shared political philosophies at a time in which zero-sum politics are rife and global powers are competing. Incentives toward global norms to protect the open Internet and to keep it secure will rather be driven by an understanding of areas of mutual dependence on the security and functioning of the global open Internet. An attack on the core infrastructure will hurt all connected to it.

Cyberspace is not independent, as J. P. Barlow declared it to be, nor is it detached from the real, physical world. People feel the impact of attacks and fragmentation. Given the rapid developments of technologies, the growing stakes of nation-states, and the increasingly important role of the private sector, the need for a rules-based online order has never been greater.

The historic guardians of the rules-based order, the United States and European countries, are well positioned to take the lead but do not seem to prioritize this ambition. At the same time, alternatives are being developed, so the choice is not between regulation or no regulation but between different values, models, and interests that will dominate the norms governing the online sphere. The private sector is increasingly pushing its norms, top-down and authoritarian governance models are gaining ground, and consensus at the UN level is becoming increasingly difficult. The absence of a rules-based frame means there is little accountability for aggressive behavior in cyberspace, yet lawlessness and fragmentation must not be the new normal. For users worldwide, the protection of the public interest of a secure and open Internet cannot be underestimated. Leadership toward protecting that public interest from attacks, profit models, or norms that are based on sovereignty rather than an open model is essential. A secure and open Internet needs an order based on rules and the rule of law to survive.

Given the rapid developments of technologies, the growing stakes of nation-states, and the increasingly important role of the private sector, the need for a rules-based online order has never been greater.

Notes

1. John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation,* last modified February 8, 1996, https://www.eff.org/cyberspace-independence.
2. Hillary Rodham Clinton, "Remarks on Internet Freedom," US Department of State, last modified January 21, 2010, https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.
3. Ibid.
4. "Digital Agenda: Karl-Theodor zu Guttenberg

Invited by Kroes to Promote Internet Freedom Globally," European Commission, last modified February 19, 2018, http://europa.eu/rapid/press-release_IP-11-1525_en.htm.
5. Ibid.
6. Evgeny Morozov, "The 20th Century Roots of 21st Century Statecraft," *Foreign Policy*, September 7, 2010, http://foreignpolicy.com/2010/09/07/the-20th-century-roots-of-21st-century-statecraft/.
7. Marietje Schaake, "Follow-up on the No Disconnect Strategy," European Parliament, last modified August 19, 2015, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2015-011923+0+DOC+XML+V0//EN.
8. David Kaye, "How Europe's New Internet Laws Threaten Freedom of Expression," *Foreign Affairs*, December 18, 2017, https://www.foreignaffairs.com/articles/europe/2017-12-18/how-europes-new-internet-laws-threaten-freedom-expression.
9. "The Spy Merchants," Al Jazeera, April 10, 2017, https://www.aljazeera.com/investigations/spy-merchants.html.
10. Communication from the United States to the WTO, "Measures Adopted and under Development by China Relating to Its Cybersecurity Law," September 25, 2017, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=238967,235083,234683,234548,233628,233629,232625,229594,229263,228945&CurrentCatalogueIdIndex=0&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=False.
11. "A Closer Look at China's Cybersecurity Law—Cybersecurity, or Something Else?," Access Now, December 13, 2017, https://www.accessnow.org/closer-look-chinas-cybersecurity-law-cybersecurity-something-else/.
12. Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution, Aegis Paper Series*, no. 1703, 2017, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.
13. Jason Healey, "The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers," *Colombia Journal of International Affairs*, November 1, 2016, https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process.
14. Adam Segal, "Tracking State-Sponsored Cyber Operations," *Council on Foreign Relations*, November 6, 2017, https://www.cfr.org/blog/tracking-state-sponsored-cyber-operations.
15. "Warsaw Summit Communiqué," NATO, last modified July 9, 2016, https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf.
16. Peter Baker, "White House Penalizes Russians over Election Meddling and Cyberattacks," *New York Times*, March 15, 2018, https://www.nytimes.com/2018/03/15/us/politics/trump-russia-sanctions.html?rref=collection%2Fnewseventcollection%2FThe%20Trump%20White%20House.
17. Nicole Perlroth and Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," *New York Times*, March 15, 2018, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.
18. George Kurtz, "CrowdStrike's 2018 Global Threat Report Reveals the Trends, Insights and Threat Actors You Need to Know," CrowdStrike, February 26, 2018, https://www.crowdstrike.com/blog/crowdstrike-2018-global-threat-report-reveals-the-trends-insights-and-threat-actors-you-need-to-know/.
19. Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (2011): 28.
20. Marietje Schaake and Mathias Vermeulen, "Towards a Values-Based European Foreign Policy to Cybersecurity," *Journal of Cyber Policy* 1, no. 1 (February 2016).
21. "Signing Pledge to Fight Cyberattacks, 34 Leading Companies Promise Equal Protection for Customers Worldwide," Cybersecurity Tech Accord, last modified April 17, 2018, https://cybertechaccord.org/.
22. Vint Cerf, "Rebuild Internet Governance before It Is Too Late," *Financial Times*, February 20, 2018.
23. Sorin Ducaru, "Absent at Munich: Placing Cybersecurity on the Main Stage of Geopolitics," *Defense News,* March 1, 2018, https://

www.defensenews.com/smr/munich-security-forum/2018/03/01/absent-at-munich-placing-cybersecurity-on-the-main-stage-of-geopolitics/.
24. António Guterres, "Address at the Opening Ceremony of the Munich Security Conference," United Nations, last modified February 16, 2018, https://www.un.org/sg/en/content/sg/speeches/2018-02-16/address-opening-ceremony-munich-security-conference.
25. Michael Schimtt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms," *Just Security*, last modified June 30, 2017, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.
26. Wolfgang Kleinwachter, "Ein Wettrüsten, das nur Verlierer kennt," *Frankfurter Allgemeine Zeitung*, February 15, 2018, http://www.faz.net/aktuell/feuilleton/debatten/die-digitalen-probleme-erinnern-an-die-siebziger-15448961.html.
27. Joseph S. Nye Jr., "Cyber Power," in *The Future of Power in the 21st Century* (Cambridge, MA: Public Affairs Press, 2011), https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf.