The Internet of Things as a Global Policy Frontier

Laura DeNardis[†][*] *& Mark Raymond*[**]

TABLE OF CONTENTS

I. CYBER PHYSICAL SYSTEMS RISE ON THE INTERNATIONAL INTERNET GOVERNANCE AGENDA

An attack on the Internet is no longer merely about disrupting communication systems connecting people, but about disrupting real-world, material infrastructure necessary for basic societal functioning. Cybersecurity concerns that were once primarily about data security, privacy, and free speech are now concerns about human safety and the operational preservation of industrial and financial infrastructure. In the summer of 2017, a cyber attack targeted Ukrainian government

[*] Laura DeNardis is a Professor in the School of Communication and Faculty Director of the Internet Governance Lab at American University.

[**] Mark Raymond is the Wick Cary Assistant Professor of International Security, as well as the Director of the Cyber Governance and Policy Center, at the University of Oklahoma.

and industrial sites in advance of a national Ukrainian Constitution holiday.[1] An online posting by the Ukrainian Infrastructure Minister acknowledged that energy companies, gas stations, railroads, the airport, and other critical infrastructure were affected.[2] The attack spread internationally and received a great deal of media and public attention, but was just one in a series of infrastructure attacks, such as the similar cyber attack years earlier that caused a Ukrainian power distribution outage.[3]

Cyber physical systems, colloquially called the Internet of Things ("IoT"), are not only potential targets, but also attack vectors from which to launch new types of cyber disruptions. In the fall of 2016, the largest botnet attack in the history of the Internet was carried out by hijacking millions of home appliances, such as security cameras and digital video recorders, and using these devices to launch a massive Distributed Denial of Service ("DDoS") attack.[4] The DDoS attack disrupted high profile websites, including Amazon and Reddit, by targeting the provider of managed Domain Name System ("DNS") services responsible for resolving domain name queries for these and other popular sites.[5] A DDoS attack hijacks unwitting devices, implements malicious code, and uses these hijacked devices to flood the targeted site with so many requests as to render the site inaccessible to legitimate traffic. The hijacked devices were trivial to infect because they had known security vulnerabilities (in Mirai source code) or weak default passwords.[6] The attack's approach of co-

[1] *See, e.g.*, Christian Borys, *The Day a Mysterious Cyber-Attack Crippled Ukraine*, BBC (July 4, 2017), http://www.bbc.com/future/story/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine.

[2] *See, e.g.*, Nicole Perlroth et al., *Cyberattack Hits Ukraine Then Spreads Internationally*, N.Y. TIMES (June 27, 2017), https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

[3] *See generally* Indus. Control Sys. Cyber Emergency Response Team (ICS-CERT), *Alert (IR-Alert-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure*, U.S. DEP'T HOMELAND SECURITY (Feb. 25, 2016), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[4] *See generally* U.S. Comput. Emergency Response Team (US-CERT), *Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets*, U.S. DEP'T HOMELAND SECURITY (Oct. 14, 2016), https://www.us-cert.gov/ncas/alerts/TA16-288A.

[5] The affected DNS provider was a company called Dyn. Its Chief Strategy Officer described the outage as "a sophisticated, highly distributed attack involving tens of millions of IP addresses . . . across multiple attack vectors and Internet locations." Kyle York, *Dyn Statement on 10/21/2016 DDoS Attack*, ORACLE + DYN (Oct. 22, 2016), http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack.

[6] *See, e.g.*, Michael Kan, *DDoS Attack on Dyn Came from 100,000 Infected Devices*, COMPUTER WORLD (Oct. 26, 2016, 2:21 PM), http://www.computerworld.com/article/

opting the Internet's underlying infrastructure, the Domain Name System, is part of what is recognized as the increasing "turn to infrastructure in Internet governance," the co-opting of infrastructures of Internet governance to achieve political or economic objectives.[7]

The "Internet of Things" is a tepid conceptual phrase designed to characterize this major transformation in the evolution of the Internet: its expansion beyond communication between people, or between people and information content, and into billions of everyday objects. IoT systems involve the acquisition of sensor data from, and the delivery of instructions to, devices that interface with or are part of the real world. The Internet of Things is often equated with home appliances and consumer devices, like wearable technologies and cars. Therefore, much initial policy concern has focused on consumer products.[8] Attention to this phenomenon is appropriate for many reasons. More Internet traffic already connects things than people, and global projections of the economic impact of the IoT is potentially eleven trillion dollars by 2025.[9] It is also appropriate because the expansion of the Internet into everyday objects used by people creates unprecedented public interest questions about how it will also transform privacy and human security.

This attention to consumer products misses the bulk of how the Internet has expanded into everyday objects. Outside of consumer IoT applications are the cyber physical systems that underlie almost all industrial sectors.[10] Gas and oil companies rely upon digitally connected energy sensors.[11] Transportation and shipping companies use Internet technologies for tracking vehicles and packages. Medical

3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html.

[7] *See generally* THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE (Francesca Musiani et al. eds., 2016).

[8] *See, e.g.*, *FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks*, FED. TRADE COMM'N (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices (urging companies to "adopt best practices to address consumer privacy and security risks").

[9] James Manyika et al., *Unlocking the Potential of the Internet of Things*, MCKINSEY & CO. (Jun. 2015), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[10] *See generally* OECD DIRECTORATE FOR SCIENCE, TECH. & INNOVATION, THE INTERNET OF THINGS: SEIZING THE BENEFITS AND ADDRESSING THE CHALLENGES (May 24, 2016), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En.

[11] *See, e.g.*, The Globe and Mail, *Roughnecks, Armed with Tablets, Transform the Energy Industry*, GE REPORTS (Sept. 3, 2015), https://gereports.ca/roughnecks-armed-tablets-transform-energy-industry.

systems increasingly rely upon Internet-connected monitoring, diagnostic, and treatment devices. Manufacturing companies use digital networks to manage the handling of materials, optimization of inventories, and connection of robotic systems. Local governments are increasingly an important IoT constituency in that street lights, utilities, traffic control systems, and other so-called smart city applications are now part of the Internet ecosystem. All economic sectors, from agriculture to retail, are now domains in which cyberspace touches the material world.[12] All of these networks, while often using some proprietary technologies, also rely on the underlying protocols and network equipment of the Internet or connect into the Internet for administration and control functions.

Whether consumer objects or the cyber physical systems of industry, the primary argument of this paper is that the Internet of Things is not merely a local jurisdiction, or even domestic issue, but an international Internet governance concern. While global debates about Internet governance have focused on contentious issues — such as the transition of U.S. oversight of the Internet's Domain Name System to the Internet Corporation for Assigned Names and Numbers ("ICANN") and a host of other content-related issues, from massive systems of censorship in China to the right to be forgotten ruling in the European Union to intellectual property concerns over piracy — global policy questions about cyber physical systems require more attention. Because the materiality of these systems has such an obvious circumscribed physical presence, it can seem like a local policy issue. The purpose of this paper is to identify a collection of emerging global public interest concerns around the IoT, paying particular attention to intersections with geopolitical and global governance concerns. We suggest that public interest concerns can be divided into the following five categories:

- Critical Internet Resource Constraints
- Privacy Complications
- Human Security
- International Security
- Global Competition Tensions

[12] For information about IoT applications in the various industry sectors mentioned here, see, for example, INT'L TELECOMMS. UNION & CISCO, HARNESSING THE INTERNET OF THINGS FOR GLOBAL DEVELOPMENT 5 (Jan. 2016), https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf.

The paper seeks to make several contributions. First, it creates a taxonomy for understanding key emerging areas of global tech policy in light of IoT trends. Second, it explains how IoT deployment in each of these areas raises global Internet governance questions (as opposed to viewing the Internet of Things as a local issue). Finally, it suggests a set of emerging analytical themes that traverse these policy areas, some of which call into question longstanding norms in global Internet governance. For example, how does multistakeholder governance apply to cyber physical systems? Is IoT fragmentation necessarily problematic or can it serve as a check on widespread cybersecurity attacks and mass data collection practices? Ultimately, the paper seeks to identify emerging international policy concerns arising from the proliferation of cyber physical systems to hopefully contribute to global policy discussions with critical implications for human rights, innovation, and security.

II. A FRAMEWORK FOR GLOBAL PUBLIC INTEREST CONCERNS IN CYBER PHYSICAL SYSTEMS

It was once a mantra in cyber policy circles that no bullets would ever be fired in cyberspace. Internet public policy concerns primarily revolved around content: intellectual property rights, freedom of expression, defamation, decency and morality, and data privacy. The material world interface of cyber physical systems is dramatically shifting the nature of public policy concerns. The ability to accommodate the growth of IoT innovations with sufficient privacy, security, and reliability is now a public policy concern with implications for human safety and basic societal functioning, as well as the preservation of the global digital economy and public sphere. Cyber physical systems are not entirely new in that they build on existing technologies and applications, but they nevertheless create new dimensions of transnational public policy challenges. This section introduces some of these core cross-border public interest concerns.

A. Critical Internet Resource Constraints

The potentially massive scale of everyday objects connected to the Internet raises pressing questions about whether shared critical Internet resources necessary for connectivity will meet these growth demands. Already measured in billions, projections for IoT growth forecast approximately twenty billion Internet Protocol connected devices by 2020.[13] In the same way that oil and water are scarce physical resources in the natural world, virtual identifiers and electromagnetic spectrum are necessary, and sometimes scarce, resources in the digital realm. Each object connected to the Internet requires a virtual identifier, traditionally an Internet Protocol ("IP") address. Most objects are connected wirelessly so also require electromagnetic spectrum. A significant policy concern is whether the infrastructure of the Internet, including critical virtual resources, will accommodate the technological transformation to ubiquitous cyber physical systems.

The distribution and administration of the shared critical Internet resources ("CIRs") necessary to access the public Internet are a cyber physical system concern with particular transnational governance dimensions. Definitions of CIRs vary, but the term usually refers to virtual shared digital resources, meaning logical rather than physical infrastructure.[14] In the realm of global Internet governance, CIRs include names and numbers, the globally unique binary and alphanumeric identifiers that serve as the Internet's address system. For example, IP addresses are unique binary identifiers that each device using the Internet requires, either assigned permanently or temporarily for a session. Binary identifiers called Autonomous System Numbers are assigned to networks, autonomous systems that conjoin to form the global Internet and agree to exchange data using Border Gateway Protocol.

Given that cyber physical systems rely heavily on wireless access, electromagnetic spectrum availability and allocation policy is a crucial concern. The proliferation of cellular telephony and other spectrum dependent services and applications face the constraints of electromagnetic frequency spectrum.[15] Some frequency bands are allocated under formal licenses and other bands are available as part of license-exempt spectrum (e.g., frequencies used by Bluetooth and Wi-Fi). The ability to quickly introduce new services and products, and

[13] For example, Cisco projects that there will be 26.3 billion IP-connected devices by 2020. *See Cisco Visual Networking Index Predicts Near-Tripling of IP Traffic by 2020*, CISCO (Jun. 7, 2016), https://newsroom.cisco.com/press-release-content?type=press-release&articleId=1771211. Gartner Group makes a similar projection of 20 billion devices by 2020. *See Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent from 2015*, GARTNER (Nov. 10, 2015), http://www.gartner.com/newsroom/id/3165317.

[14] LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE 36 (2014).

[15] Shamika Ravi & Darrell M. West, *Spectrum Policy in India*, CTR. FOR TECH. INNOVATION AT BROOKINGS 1 (Aug. 2015), https://www.brookings.edu/wp-content/uploads/2016/06/Spectrum-Policy-in-India8515.pdf.

compete and innovate in the fast moving IoT space, is aided by the ability to use expeditious license-exempt spectrum. As cyber physical systems and other heavily wireless-dependent applications proliferate, spectrum resource constraints are likely to become a global policy concern.

IP address constraints are another CIR policy concern for cyber physical systems. To be locatable and reachable, objects require a virtual address. While addressing approaches for sensor networks, IoT environments, and other cyber physical systems is complicated by usage of proprietary protocols and addressing spaces and Network Address Translation ("NAT"),[16] IP addresses are a critical resource requirement. As such, the collective action problem and global governance issue of IPv6 adoption is of particular importance to the future of cyber physical systems. The IP address space (i.e., the number of available binary addresses) under the prevailing IPv4 standard is entirely allocated, and nearly entirely assigned. This standard assigns 32 bits (0s and 1s) to each address so enables a total of 2^{32}, or approximately 4.3 billion addresses, an insufficient number to support the growth of the Internet. The newer standard IPv6 expands the address length to 128 bits, providing a massive pool of 340 undecillion addresses but, in part because it is not natively backward compatible with IPv4, is still not widely adopted. Growth in IPv6 adoption will be a critical enabler of consumer IoT advancement. In other cases, having non-interoperable cyber physical systems based on IPv6 or even a completely proprietary addressing standard may be desirable as a way to bolster security of critical infrastructure.

These resource availability concerns and complexities also raise issues for Internet governance norms, including the stability and necessity of CIR administration in global Internet governance institutional structures. One definition of the Internet has often been based on the use of the Internet Protocol and predicated upon a structure of a shared universal address space in which the requirement for global uniqueness in logical identifiers led to a particular form of centralized coordination.[17] Does an object in the Internet of Things

[16] Network Address Translation is a technique that enables devices on a private network to share a single public IP address via a gateway between the private network and the public Internet.

[17] Among others, network designers in the Internet Engineering Task Force ("IETF") have historically viewed the ability to be reached via the Internet Protocol ("IP") as defining whether one was on the Internet. *See, e.g.*, David D. Clark et al., *Towards the Future Internet Architecture*, INTERNET ENG'G TASK FORCE (Dec. 1991), https://www.ietf.org/rfc/rfc1287.txt.

always require an IP address? Does the DNS have as central of a role if objects are connected rather than traditional content-mediating computers? In the world of RFID tags, Bluetooth, and resurging proprietary networks, it is reasonable to assume that not every object will have its own IP address. Local networks can communicate with local systems of addressing and connect to the public network via a gateway device that uses an IP address. The role of names and numbers coordinating institutional structures potentially diminishes in this context. The notion of a universal Internet not requiring a universal name and binary address space is radical in light of the historical technological and administrative trajectory of critical Internet resources.

Global Internet resource concerns also foreshadow various themes that arise across the other categories of public policy challenges we identify in this paper. These themes include: (1) challenging the notion of a universal Internet based on a universal name and number space and (2) determining what multistakeholder governance looks like in environments in which private companies make design and governance concerns inside of proprietary technical ecosystems that may not involve government, civil society, or new global institutions like ICANN, the global multistakeholder organization overseeing Internet names and numbers.

B. Privacy Complications

The Internet of Things expands conceptions of privacy far beyond personal communication and information knowingly exchanged between humans, and metadata around this content, to the more pervasive sphere of everything individuals do in their homes, jobs, cars, and even in public places. Corporate data collection is potentially more massive, pervasive, and invasive, but many relevant companies do not even have privacy terms of service. The private data collection of everyday objects and activities heightens opportunities for government surveillance of these everyday activities, whether for law enforcement, domestic or foreign intelligence gathering, or politically motivated tracking of dissidents and media. Similar concerns arise from the deployment of cyber physical systems that collect data by local governments, such as police body cameras and traffic monitoring systems.

Data gathering practices around cyber physical systems raise traditional privacy questions such as what data is gathered and how is it used? Who sees it? How is it retained and for how long? How is it stored? To what extent is it personalized or anonymized? Is it encrypted in transit and at rest? Under what conditions will corporations be lawfully required to share consumer data with governments?

Cyber physical systems also raise different-in-kind concerns. In particular, consent is complicated. IoT devices (e.g., some wearables, smart city sensors, and Internet-connected toys) sometimes have no display screen. Conveying or updating a privacy policy or consenting to terms of service is not easily possible without a screen. Individuals may not even be aware of the ambient data collection of physical IoT devices. This may be the case for consumers who have installed the products, but certainly for others unwittingly in proximity to the device's data collection practices. For example, toys embedded with microphones and voice recognition software can pick up ambient conversations of those not even aware of these features, as an FBI public service announcement warned in 2017.[18]

Concerns around privacy and surveillance top government policy interest in the IoT. The European Commission has engaged in public consultation and published output from IoT working groups, with a strong overlay of concern for consumer privacy.[19] The United States Federal Trade Commission ("FTC") issued a 2015 staff report specifically addressing IoT privacy and security.[20] The 36th International Conference of Data Protection and Privacy Commissioners issued the "Mauritius Declaration on the Internet of Things," including a strong statement on the need for IoT privacy from the outset: "Data processing starts from the moment the data are collected. All protective measures should be in place from the outset. We encourage the development of technologies that facilitate new ways to incorporate data protection and consumer privacy from the outset. Privacy by design and default should no longer be regarded as something peculiar. They should become a key selling point of innovative technologies."[21]

[18] *Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children*, FBI (July 17, 2017), https://www.ic3.gov/media/2017/170717.aspx.

[19] *Conclusions of the Internet of Things Public Consultation*, EUR. COMM'N (Feb. 28, 2013), https://ec.europa.eu/digital-single-market/news/conclusions-internet-things-public-consultation.

[20] *See generally* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[21] INT'L CONFERENCE OF DATA PROT. & PRIVACY COMM'RS, MAURITIUS DECLARATION ON THE INTERNET OF THINGS 2 (Oct. 14, 2014), https://edps.europa.eu/sites/edp/files/publication/14-10-14_mauritius_declaration_en.pdf.

Despite this policy interest in privacy, Internet of Things markets and associated privacy approaches are a highly privatized and quickly moving sphere. Whether implemented in industrial settings, homes, or municipalities, product manufacturers are private companies. Because of the rapid pace of innovation and product development in this space, often preceding applicable regulations, there may not be sufficient market incentives to provide the security necessary to create strong privacy. On the other hand, consumer trust in IoT system privacy, as well as security and safety, is likely to correlate to market acceptance and IoT growth. Cyber physical system markets do not yet have trust architectures such as privacy policy terms of service, transparent practices around personal data disclosure, consumer choice for opting out of data collection, or data breach notifications.[22]

It is sometimes unclear whether prevailing privacy guidelines around content intermediaries or in industry-specific settings such as banking and healthcare — whether voluntary, recommended, or statutory — apply to cyber physical systems. These companies produce real-world rather than virtual products, but have the same type of data intermediating role as traditional information intermediaries such as Google, or financial intermediaries such as banks. The Organisation for Economic Co-operation and Development ("OECD") updated its "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" in 2013.[23] Some of the most reasonable recommendations made to data controllers — such as around accountability, plans for responding to incidents, notification of data breaches, and the provision of appropriate safeguards — are not at all the norm among IoT companies.[24]

What raises the stakes considerably is that an infiltration of data in cyber physical systems can result in loss of human life and loss of basic day-to-day functioning, not just loss of communication data. Privacy is now related to human security, addressed next.

C. *Human Security*

The concept of human security, in contrast to traditional international relations treatments of national (state) security, emerged

[22] OFFICE OF THE PRIVACY COMM'R OF CAN., THE INTERNET OF THINGS: AN INTRODUCTION TO PRIVACY ISSUES WITH A FOCUS ON THE RETAIL AND HOME ENVIRONMENTS (Feb. 2016), https://www.priv.gc.ca/media/1808/iot_201602_e.pdf.

[23] ORG. FOR ECON. COOPERATION & DEV., THE OECD PRIVACY FRAMEWORK 11-18 (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[24] FED. TRADE COMM'N, *supra* note 20.

after the Cold War. Proponents sought to reconceptualize security as dealing not only with military threats to states by other states, but also with non-military threats experienced by individuals and groups.[25] Despite the benefits of such an approach, the expansive definition of human security created analytical problems and left policymakers "little guidance in the prioritization of competing policy goals."[26] The United Nations Development Programme defined human security as having two primary components: (1) "safety from such chronic threats as hunger, disease and repression" and (2) "protection from sudden and hurtful disruptions in the patterns of daily life — whether in homes, in jobs or in communities."[27]

We accept that securing basic civil and political rights is essential to ensuring acceptable quality of life for individuals. We further accept that securing basic civil and political rights is instrumental to ensuring the physical security of individuals, including from their own states. The use of online surveillance, which can be magnified by employing cyber physical systems, to identify and target dissidents has become all too familiar.[28] However, widespread deployment of cyber physical systems can also create direct physical threats to individuals and groups. It is this narrower subset of human security concerns that we highlight in this section.

Some such concerns arise from consumer-facing manifestations of cyber physical systems. These include product liability issues created by autonomous vehicles and household products that can affect individual safety. In the event that software flaws or hacked systems are responsible for injury or death, for example, there may be complications around holding firms responsible given the weakness of software liability laws, especially where the software was purchased by the device manufacturer from a different firm. Such concerns have not typically been seen as human security issues, as domestic legal systems in industrialized states are accustomed to dealing with personal injury and product liability cases; however, as cyber physical systems are brought to market at global scale by firms across a wide variety of industrial sectors, consumers in emerging markets may have difficulty

[25] *See generally* Roland Paris, *Human Security: Paradigm Shift or Hot Air?*, 26 INT'L SECURITY 87, 98-100 (2001).

[26] *Id.* at 88.

[27] UNITED NATIONS DEV. PROGRAMME, HUMAN DEVELOPMENT REPORT 22 (1994), http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf.

[28] *See generally* RONALD DEIBERT ET AL., ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE (2010).

effectively utilizing civil court systems in the jurisdictions where major global firms are headquartered.

The most serious human security concern associated with cyber physical systems pertains to injury or loss of life from disruption to key cyber physical systems such as electrical grids, health systems, and transportation systems. These disruptions may be the result of: (1) targeted attacks against the cyber physical systems themselves; (2) collateral damage from cyberattacks that target unrelated computer systems, including critical Internet infrastructure, but that affect computer systems on which the cyber physical systems rely; or (3) malfunctions of various kinds. All of these kinds of disruptions pose transnational challenges. To the extent these cyber physical systems are operated by firms in other jurisdictions, or subcontract computer support services to firms outside local jurisdictions where they are deployed, responding to disruptions will require transnational coordination. Even more challenging, these complex contractual relationships may be opaque to first responders and appropriate authorities in times of emergency, hampering response times. Given long expected lifecycles for devices in the utilities and infrastructure sectors, there will likely also be significant updating challenges both for hardware and firmware, as well as associated control software.

Existing national and international efforts to deal with critical infrastructure have focused on hardening, in other words, securing, critical systems,[29] and on the creation of global norms against deliberately targeting these systems.[30] While these efforts are important, and should be pursued, there are good reasons to expect that they will not be sufficient. First, the ease of offense and difficulty of defense in the cyber domain suggests that even critical systems will be very difficult to sufficiently harden.[31] Second, the importance of power grids and transportation infrastructure to military effectiveness suggests that the temptation to attack them in the case of armed conflict will be extremely strong. Indeed, Russian efforts to destabilize Ukraine suggest that some states are already employing such tools as

[29] *See* Hans Brechbühl et al., *Protecting Critical Information Infrastructure: Developing Cybersecurity Policy*, 16 INFO. TECH. FOR DEV. 83, 83-84 (2010); Scott J. Shackelford & Zachery Bohm, *Securing North American Critical Infrastructure: A Comparative Case Study in Cybersecurity Regulation*, 40 CAN.-U.S. L.J. 61, 65 (2016).

[30] On global cybersecurity norms, including for critical infrastructure, see Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 426 (2016).

[31] *See generally* Joseph S. Nye, Jr., *Nuclear Lessons for Cyber Security?*, STRATEGIC STUD. Q., Winter 2011, at 18.

part of a 'hybrid warfare' approach, even in situations short of open armed conflict.[32] The effects of such attacks will almost certainly spill over to affect civilians, creating significant human security costs.

These emerging realities raise major questions about who is responsible for providing security to whom. While the state has been understood as the primary guarantor of its citizens' physical safety, the unfortunate reality is that many states are in fact the most dangerous threat to their own citizens. Further, scholars have noted an apparent shift toward private security provision.[33] Elke Krahmann has argued that the commodification of security tends to skew security provision in patterned ways. Notably, it tends to encourage provision of reactive rather than preventive security services, so as to ensure an ongoing market that would be absent if the threat were eliminated. Further, it tends to encourage overprovision of certain types of security services — namely those that provide excludable benefits on which price mechanisms depend, as well as those tailored to the needs of those with the greatest ability to pay. As a result, private security provision tends to lead to the more narrow distribution of security across income levels, as well as to a security landscape characterized by mitigation and remediation of damage, rather than prevention.[34] Cybersecurity provision is perhaps more privatized than any other segment of the security landscape, and the general conditions in this market are consistent with Krahmann's argument.

Given the traditional role of the state, it is not clear whether governments or citizens will continue to tolerate highly privatized cybersecurity provision in the event that injury and loss of life from disruption of critical cyber physical systems becomes commonplace. One possibility is that states will continue to expand their interventions into this policy space, furthering the trend toward a more fragmented Internet that Demchak and Dombrowski provocatively called a 'cyber Westphalia.'[35] Such an outcome raises several of the themes that we expand upon in the next major section

[32] While this approach has been called the "Gerasimov doctrine," Mark Galeotti notes that the approach bears similarity both to earlier Russian warfighting ideas and to Western practices. *See* Mark Galeotti, *Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?*, 27 SMALL WARS & INSURGENCIES 282, 282 (2016).

[33] This is arguably part and parcel of what Susan Strange famously called "the retreat of the state." *See generally* SUSAN STRANGE, THE RETREAT OF THE STATE: THE DIFFUSION OF POWER IN THE WORLD ECONOMY (1996).

[34] *See generally* Elke Krahmann, *Security: Collective Good or Commodity?*, 14 EUR. J. INT'L REL. 379 (2008).

[35] *See generally* Chris C. Demchak & Peter J. Dombrowski, *Rise of a Cybered Westphalian Age: The Coming Decades*, STRATEGIC STUD. Q., Spring 2011, at 31, 34.

of the article, including jurisdictional complexity, market failure, fragmentation as a malleable value, and the appropriateness of private and multistakeholder governance modalities for cyber physical systems.

D. *International Security*

Widespread global deployment of cyber physical systems also raises important policy challenges in the realm of international security. The underlying pattern, noted above, is that a world in which cyber physical systems are essential to virtually every domain of human life and the global digital economy significantly increases the number of valued referent objects that must be secured from potential attacks, and also greatly expands the potential sources of such attacks. Defenders must protect a far greater number of devices from many more attack vectors. This kind of situation has been understood as dangerous, because actors convinced that the current state of technology confers a decisive advantage to the attacker are especially prone to escalate crises.[36]

Two recent analyses add important nuance to discussions of offense dominance in the cyber domain and the prospects for deterrence. Rebecca Slayton argues that general assessments of the balance should be avoided in favor of more granular assessments. Further, she argues that any such balance depends not only on the state of technology, but also on "the organizational processes that govern interactions between technology and skilled actors."[37] Because these organizational variables differ by actor, the cyber offense-defense balance must be assessed dyadically (that is, between specific pairs of potential attackers and defenders) rather than systemically. In addition, Slayton argues that organizational variables tend to diminish the actual advantages enjoyed by attackers.[38] Joseph Nye notes that deterrence need not depend fully on retaliatory threats, and that it can also be enhanced by strategies of defense (hardening targets to make them less attractive to attackers), entanglement (costs imposed on the attacker due to interdependence), and norms that prohibit exploiting offensive advantages or otherwise engaging in retaliatory conduct. He

[36] *See generally* Robert Jervis, *Cooperation Under the Security Dilemma*, 30 WORLD POL. 167 (1978); Stephen Van Evera, *The Cult of the Offensive and the Origins of the First World War*, 9 INT'L SECURITY 58 (1984).

[37] Rebecca Slayton, *What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment*, INT'L SECURITY, Winter 2016/17, at 72, 74.

[38] *See id.* at 107.

recommends that policymakers direct attention primarily to the most serious potential attacks, and that they make use of all these strategies to manage international security threats in the cyber domain.[39]

The overall effect of ubiquitous cyber physical systems on international security remains unclear. On the one hand, "the advantages that complex software offers attackers diminish rapidly at the 'edges' of cyberspace, where computers are used to control physical systems, because knowledge of the physical systems is needed to exercise careful control."[40] On the other hand, such technology "greatly expands the attack surface and blurs the boundaries of the systems whose resilience needs to be enhanced."[41] It is undeniable that as more aspects of more societies become more reliant on computer networking — including for essential monitoring and remote control functions — states will confront a greater variety of vulnerabilities arising from the cyber domain. Many of these will entail risks to citizens in their civilian capacities and therefore might be understood primarily as human security concerns. However, researchers affiliated with the NATO Cooperative Cyber Defence Centre of Excellence have indicated that attacks in Ukraine and elsewhere, widely believed to have been conducted by or at the behest of the Russian government, can be understood as internationally wrongful acts and violations of state sovereignty under the customary international law of state responsibility and the United Nations Charter.[42] While not an official position either of NATO or any of its individual member states, such quasi-official interpretive statements are indicative of norm construction efforts in this area by Western democracies.

Regardless of whether a candidate norm against attacks like NotPetya or WannaCry becomes widely adopted among states, these efforts are likely to inform NATO decision-making in the cyber domain. If major powers adopt differing conceptions of the norms applicable to state military use of information and communication technologies ("ICTs"), these differing interpretations of legitimate behavior could themselves become sources of conflict — which would likely play out in large part within the cyber domain. This is because consistent state practice is a central element in the formation and

[39] *See* Joseph S. Nye, Jr., *Deterrence and Dissuasion in Cyberspace*, INT'L SECURITY, Winter 2016/17, at 44.

[40] Slayton, *supra* note 37, at 107.

[41] Nye, *supra* note 39, at 57.

[42] *See generally NotPetya and WannaCry Call for a Joint Response from International Community*, NATO COOPERATIVE CYBER DEF. CTR. EXCELLENCE (Jun. 30, 2017), https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html.

determination of rules of customary international law. This feature of the international system underlies a variety of state behavior, such as the Russian effort to place a flag on the seafloor in the high Arctic,[43] Canadian and Danish efforts to establish even minimal evidence of sovereignty over Hans Island,[44] and naval deployments to contested areas of the ocean.[45] In the future, states may conduct attacks simply to preserve the legal argument that a particular kind of cyber operation is legal, or in any event not expressly prohibited, under international law. Such arguments would likely be met with skepticism by much of the international community, but could be advanced by a small handful of outlier states.

Apart from disputes that might arise from such efforts to preserve freedom of action by publicly contravening a candidate norm, and the likely use of offensive cyber capabilities in the event of armed conflict, states are almost certain to make continued use of opportunities associated with cyber physical systems for espionage purposes. These espionage activities comprise a spectrum from passive information collection (e.g., about traffic patterns on highways or public transportation, about electricity consumption patterns, and the capacity of other energy systems such as pipelines) to what Thomas Rid has called subversion operations that seek "to undermine the authority, the integrity, and the constitution of an established authority or order."[46] Cyber physical systems are likely to offer state actors important opportunities in pursuit of both of these kinds of operations.

Since subversion operations target human opinion rather than computer systems, it is likely that cyber physical systems will play only a supporting role in such scenarios; however, it is not difficult to imagine at least two significant ways in which they might do so. First, subversion operations are likely to benefit from information about the intended audience. The more such propaganda content can be tailored and targeted, the more likely it will resonate with recipients; like spearphishing attacks delivered via emails designed to mislead the recipient into believing they are benign, subversion is enhanced by

[43] *See* C.J. Chivers, *Russians Plant Flag on the Arctic Seabed*, N.Y. TIMES (Aug. 3, 2007), http://www.nytimes.com/2007/08/03/world/europe/03arctic.html.

[44] Dan Levin, *Canada and Denmark Fight Over Island with Whisky and Schnapps*, N.Y. TIMES (Nov. 7, 2016), https://www.nytimes.com/2016/11/08/world/what-in-the-world/canada-denmark-hans-island-whisky-schnapps.html?_r=0.

[45] *South China Sea: US Carrier Group Begins 'Routine' Patrols*, BBC (Feb. 19, 2017), http://www.bbc.com/news/world-asia-china-39018882.

[46] Thomas Rid, *Cyber War Will Not Take Place*, 35 J. STRATEGIC STUD. 5, 22 (2012).

sophisticated social engineering. As cyber physical systems collect more information about individuals' daily routines and consumption patterns, political subversion campaigns can be made more potent. Second, botnets including devices associated with large cyber physical systems could be used to conduct powerful DDoS attacks designed to inhibit efforts to counter political subversion campaigns, for example by targeting Computer Emergency Response Teams and/or major media outlets. The result could be to exert temporarily enhanced control over the information environment surrounding major events like elections or geopolitical crises.

Cyber physical systems are of even more obvious utility to passive information collection efforts. This is true both at the aggregate level, in terms of providing a sense of another state's industrial and military potential, and at the individual level. As cyber physical systems become increasingly ubiquitous, the resulting data will provide a picture not only of aggregate societal patterns but also (to the extent it can be associated with particular individuals) of the activities and routines of key military and political leaders. Such information could be used to compromise and blackmail such figures, to coerce them to turn over more sensitive information, or to otherwise act at the behest of a foreign power.

To the extent that leaders perceive cyber physical systems as a source of threat — either to human or national security — they are likely to insist on exercising increased control over this policy area, and potentially also to insist on imposing controls or restrictions on the digital economy. Such restrictions might take various forms. First, they could entail restrictions on data flows related to sensitive cyber physical systems, requirements that such data be stored exclusively within the state's jurisdiction, or both. Such requirements have already been enacted in some jurisdictions and have attracted the attention of the legal profession.[47] Second, they could involve supply chain restrictions or other measures to ensure the integrity of hardware, firmware, and software deployed on a country's national network architecture or even in the private sector marketplace. In 2017, Kaspersky Labs indicated its willingness to turn over source code to the United States government, in response to efforts in the U.S. Senate to exclude Kaspersky from the American market over concerns about its potential ties to the Russian government.[48] The Russian

[47] *See generally* Courtney Bowman, *Data Localization Laws: An Emerging Global Trend*, JURIST (Jan. 6, 2017, 9:53 AM), http://www.jurist.org/hotline/2017/01/Courtney-Bowman-data-localization.php.

[48] Joe Uchill, *Kaspersky Willing to Turn over Source Code to US Government*, THE

government reportedly already requires foreign technology firms to turn over such code as a condition of market access,[49] as does China.[50]

The point is not to say that such policies are necessarily inappropriate, though requiring disclosure of source code creates what several prominent cybersecurity experts referred to as the problem of "keys under doormats" — the more keys exist, the more likely that the keys will fall into unauthorized hands.[51] Such mandated disclosures can also be used for purposes beyond the stated scope of the requirement, for example to identify vulnerabilities that can be exploited for espionage or military purposes, or to enable domestic surveillance and repression. Rather, the point is that the policy challenges associated with ICTs in general, and cyber physical systems in particular, do not exist in isolation. Solutions to one issue may exacerbate other policy challenges. Policymakers will inevitably confront tensions and tradeoffs. Further, the highly decentralized nature of Internet governance and cyber policy means that these decisions will be made by a large number of different bodies and processes with divergent values, interests, and cultures.[52]

E. Global Competition Tensions — Innovation and Interoperability Versus Enclosure

The Internet of Things, whether consumer or industrial, is thought to represent the next wave of innovation in cyberspace. The previous sections foreshadow urgent questions about the potential for ongoing innovation in emerging terrains of cyber physical systems. How will

HILL (July 2, 2017, 9:51 AM), http://thehill.com/policy/cybersecurity/340420-kaspersky-willing-to-turn-over-source-code-to-us-government.

[49] Greg Price, *U.S. Tech Companies Give Russia Secretive Source Codes to Stay in Multibillion-Dollar Market*, NEWSWEEK (June 23, 2017, 11:43 AM), http://www.newsweek.com/russia-us-tech-source-code-628589.

[50] Paul Mozur, *New Rules in China Upset Western Tech Companies*, N.Y. TIMES (Jan. 28, 2015), https://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html.

[51] HAROLD ABELSON ET AL., KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS 1 (July 7, 2015), https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8.

[52] *See generally* Mark Raymond & Laura DeNardis, *Multistakeholderism: Anatomy of an Inchoate Global Institution*, 7 INT'L THEORY 572 (2015) [hereinafter Raymond & DeNardis, *Multistakeholderism*]; Mark Raymond, *Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot*, STRATEGIC STUD. Q., Winter 2016, at 123; Mark Raymond, *Puncturing the Myth of the Internet as a Commons*, 14 GEO. J. INT'L AFF. (SPECIAL ISSUE) 53 (2013); JOSEPH S. NYE, JR., GLOBAL COMM'N ON INTERNET GOVERNANCE, THE REGIME COMPLEX FOR MANAGING GLOBAL CYBER ACTIVITIES (2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

attempts to harmonize privacy and security frameworks in cyber physical systems affect the pace of innovation? What effects will bordered national regulatory approaches have on cross-border IoT systems and companies? Will stores of critical Internet resources accommodate projected growth in the number of interconnected devices? To what extent will high-profile cybersecurity breaches, whether originating with the state or cybercriminals, erode consumer trust and market adoption in the IoT? As with other questions of Internet governance, different sets of values come into tension.

Underlying design values that have shaped global Internet growth and innovation include, among others, permissionless innovation, the ability of anyone to introduce a new service or product without requiring permission, and the principle of interoperability, the capacity for standards-based mutual exchange of information, regardless of device manufacturer or geography.[53] The primary technical enabler of these features has been the availability of open standards, technical specifications that are openly published and that have minimal, or no, underlying intellectual property constraints on their use. For most of the rapid-growth years of the Internet, the underlying standards, established for example by the Internet Engineering Task Force or the World Wide Web Consortium, have been open standards. Any new market entrant could access and use the standards to develop products that would be assured to interoperate with other hardware and software based on these standards.

IoT product ecosystems, created by firms across sectors including and far beyond ICT industries, have not aspired to implement competition-enabling open standards commensurate to content intermediating products. It can be argued, contrary to the traditions of the Internet, that there is a resurgence of market approaches in opposition to interoperability and competition. Such approaches, by design or at least in effect, lock users into proprietary ecosystems that forestall competition and maximum market innovation.[54]

[53] The Internet Society calls these, and other design principles, "Internet invariants." *See, e.g.*, *Internet Invariants: What Really Matters*, INTERNET SOC'Y (Feb. 3, 2012), https://www.internetsociety.org/internet-invariants-what-really-matters. *See generally* LESLIE DAIGLE, GLOBAL COMM'N ON INTERNET GOVERNANCE, ON THE NATURE OF THE INTERNET (2015), https://www.cigionline.org/sites/default/files/gcig_paper_no7.pdf.

[54] *See, e.g.*, PATRIK FÄLTSTRÖM, GLOBAL COMM'N ON INTERNET GOVERNANCE, MARKET-DRIVEN CHALLENGES TO OPEN INTERNET STANDARDS (2016), https://www.cigionline.org/sites/default/files/gcig_no33web.pdf (explaining this trend toward proprietary IoT approaches from an Internet engineer's perspective).

Throughout most of the history of the Internet, anti-competitive and proprietary approaches (think proprietary, non-interoperable online systems of the 1990s) have been considered regressive to innovation and open standards (e.g., TCP/IP and HTTP) have been thought to spur innovation and new product offerings.[55] When viewing cyber physical systems through an international relations lens, and in light of the other policy issues raised above, it may be the case that lack of interoperability can serve as a check on invasive surveillance, widespread cybersecurity attacks, and cyber conflict. Conversely, the argument can be made that open standards, which are typically developed in more participatory, cross-business approaches and which allow for open inspection, can have hardened security features and fewer protocol vulnerabilities than proprietary specifications which are closed in development and not open for inspection and wide technical oversight. Complicating this environment of mixed open and proprietary approaches is the question of how bordered national regulations could suppress innovation and how antitrust standards apply to the IoT.

III. CYBER PHYSICAL SYSTEM THEMES COMPLICATING TECHNOLOGY GOVERNANCE NORMS

As suggested at the outset, and despite their material presence in homes and industrial sites and other physically circumscribed settings, cyber physical systems are not a local issue any more than are other Internet applications, services, and systems a local issue. Any local-international demarcation breaks down at both technological and policy levels. Internet-connected material objects are sometimes in contention for global pools of critical Internet resources such as IP addresses and electromagnetic frequency spectrum; they involve infrastructures (systems of routing, Internet Exchange Points, cloud computing services) that can be located in other geographic regions or countries. As such, one theme is cross-jurisdictional complexity, especially for industry sectors that cross national borders or for implementations in which coders, manufacturers, standards-setting institutions, and device owners reside in different jurisdictions. Cyber physical systems have cross-border policy implications such as the potential for more invasive cross-border surveillance in private spheres, and tensions between different jurisdictional conceptions of

[55] *See generally* OPENING STANDARDS: THE GLOBAL POLITICS OF INTEROPERABILITY (Laura DeNardis ed., 2011).

personal privacy and the balance between privacy and law enforcement and intelligence gathering.

Cyber physical systems also raise the stakes of cyber governance functions necessary to keep the Internet operational. All Internet governance tasks, from standards setting to cybersecurity governance, already have significant public interest implications.[56] For example, private information intermediaries establish public policy via terms of services and privatized decisions about what counts as privacy, free speech, and morality. But cyber physical systems raise the stakes of this policy making role, whether private, public, or multistakeholder, because of the significant human security, digital economy, and national security implications of keeping systems operational and secure. Questions of risk and liability increase, as does the question of accountability and liability for systems that cross borders and include a variety of networks, services, objects and control devices.

The emerging cyber physical system policy issues identified above also help emphasize the phenomenon of the privatization of public policy in the digital sphere. The private sector — not just content intermediaries but all industries from energy to consumer goods companies — owns and operates most cyber physical systems. For example, energy companies own and operate the digital systems that connect sensors, equipment, and distribution systems. Corporate social responsibility around risk, accountability, transparency, and liability are still in flux in this technological landscape. In the context of innovation incentives to be first to market, there are not necessarily market incentives for strong cybersecurity or device upgradability. Complicating this issue is the role of artificial intelligence in risk determinations, such as the programming of driverless cars to make life and death decisions. In areas such as privacy and security, there may be little incentive for device manufacturers or IoT system providers to fully take care of security, considering the need to quickly bring products to market and quickly create new products, and uncertainty about the existence and effectiveness of legal and regulatory frameworks at the domestic and international levels. Government oversight is also highly problematic because governments have an incentive to have cyber offense as well as cyber defense capability, and an interest in environments that enable surveillance. There is a multistakeholder governance oxymoron. It is unclear what multistakeholder governance looks like in the IoT environment. Many firms deploying cyber physical systems are not, at least historically,

[56] *See generally* Raymond & DeNardis, *Multistakeholderism*, *supra* note 52.

technology firms. They have little experience with the existing legacy mechanisms for Internet governance, and in many cases may have little or no experience with multistakeholderism as a governance modality.

Finally, IoT policy concerns call into question key norms of global Internet governance, such as the objective of network universality and avoidance of Internet fragmentation. Fragmentation becomes a malleable value rather than something to always eschew for cyber-universality because lack of interoperability may have salutary effects in the context of cyber physical system security and privacy vulnerabilities. Longstanding norms of Internet governance have to be on the table for reconsideration.

CONCLUSION

Our purpose in this paper has been to survey and categorize global policy challenges associated with cyber physical systems, and to identify themes among these challenges. Resolving these challenges is beyond the scope of this paper. Indeed, we want to conclude by noting that policies to deal with cyber physical systems are likely to remain in flux for some time, as there is considerable uncertainty about the policy implications of the technology, and as the technology itself continues to evolve rapidly. In particular, the combination of cyber physical systems and machine learning is likely to create unanticipated complications for states, societies, firms, and individuals. Finally, the responses of these social actors to the technology will set off separate cycles of innovation and adaptation.

In an environment characterized by uncertainty, permissionless innovation, high interdependence, and decentralized governance, it is especially important that significant attention be paid to dispute-resolution mechanisms. Many such mechanisms exist, at the domestic and global levels. Resolving disputes is central to the work of Internet bodies such as ICANN, IETF, and W3C; states often employ international organizations for dispute resolution purposes, as with the work on norms for state military use of ICTs done by the First Committee of the United Nations General Assembly; and dispute resolution is also accomplished at the domestic level via legislatures, regulatory agencies, and courts. However, the professionals who operate such processes typically lack expertise in ICTs and cyber physical systems. Such professionals include national diplomats; international organization secretariats; judges, clerks, and attorneys at the domestic and international levels; legislators and legislative staffers at the national and subnational levels; staff at national and subnational regulatory agencies; managers and design team members at firms in technology and other industrial sectors that will increasingly be involved with deploying and operating cyber physical systems; and members of civil society organizations concerned with digital issues and with consumer protection. This list obviously encompasses a wide range and large number of individuals from across the globe. Ensuring that these individuals possess the requisite expertise to deal sensibly and appropriately with the policy implications of cyber physical systems, and the local and global policy challenges they generate, will require a substantial effort in ongoing professional education. We believe that universities, with appropriate financial and other support from the public and private sectors, are uniquely placed to convene and operate such processes. In doing so, it is essential that the skills and knowledge provided be broadly inclusive, encompassing knowledge about ethics, policy, law, and governance in addition to knowledge about engineering and computer science.

Since the private sector has such an important role in the development, deployment, and operation of cyber physical systems, we also believe it would be particularly useful to create a dedicated work stream within the United Nations Global Compact, the leading global effort to develop and implement guidelines for corporate social responsibility. Such an effort should include not just technology firms, governments, and civil society; it should also include firms that operate, or that contemplate operating, cyber physical systems as part of their regular business practices.