CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

PAPER

OCTOBER 2019

ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies

Ariel E. Levite

ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies

Ariel E. Levite

For your convenience, this document contains hyperlinked source notes indicated by teal-colored text.

Carnegie does not take institutional positions on public policy issues; the views represented herein are the author's own and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

Acronyms

CoT	Charter of Trust
CSR	corporate social responsibility
ESG	environmental, social, and corporate governance
EU	European Union
GGE	UN Group of Governmental Experts
ICS	industrial control system
ICT/OT	information and communication technology / operational technology
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
ISM	Institute for Supply Management
ISMS	information security management system
ITU	International Telecommunications Union
NIST	U.S. National Institute of Standards and Technology
NSA	U.S. National Security Agency
OECD	Organization for Economic Cooperation and Development
OEWG	Open-Ended Working Group
PLC	programmable logic controllers
VEP	U.S. Vulnerabilities Equities Process
WTO	World Trade Organization

Executive Summary

In an increasingly digitized world, information and communication technologies (ICTs), and especially operational technologies (OTs), have assumed critical importance for governments, industry, and the general public worldwide. Yet trust in the integrity of these products and services is declining because of mounting concerns over inadvertent vulnerabilities in the supply chain and intentional backdoor interventions by state and corporate actors. Compounding the problem, these legitimate security concerns are sometimes exaggerated for political and commercial reasons—a counterproductive dynamic that fuels rivalries, fragments the marketplace, increases anxiety, stifles innovation, and drives up costs.

Inarguably, some governments have been intervening in the ICT/OT supply chain or at least laying the groundwork for such interventions. They believe the pursuit to be justifiable and legal, citing objectives related to intelligence, law enforcement, and military operations. Whether valid or not, the concern is that certain corporations are actively or passively weakening the security of the supply chain and final products either at the behest of governments or for questionable purposes. Another concern is that both state and corporate interventions could leverage or mask what are purely lax security standards or flaws in products and services. And this further reduces trust in ICT/OT.

The global tumult over the integrity of Huawei products and the U.S. administration's campaign to persuade other countries to ban them exemplifies the scale of the emerging challenge. Other examples include the alleged 2015 Russian manipulation of Kaspersky Lab antivirus software being used by a U.S. National Security Agency contractor, and concerns that the agency was putting the security of U.S. products at risk. These instances illustrate the high stakes surrounding the protection of supply chains—stakes that affect geopolitics, espionage and security competition, mercantilism, and consumer protection. If concerted, cooperative efforts are not made to restore confidence in the integrity of supply chains, everyone—consumers, vendors, governments—will lose.

Many worthy, promising initiatives are underway to enhance supply chain integrity. Yet these typically approach the challenge from four stovepiped perspectives: technical, operational, commercial, and/or legal. Moreover, none of them deals head on with deliberate interventions in the supply chain. While eliminating these interventions is neither possible nor necessarily desirable, rules of the road would help restrict, channel, and condition state interventions and guide corresponding corporate behavior.

But to be effective, these rules, or obligations, should aim to enhance trust, accountability, transparency, and receptivity. They should also be anchored in existing national and international arrangements and be accompanied by measures to secure buy-in, reward compliance, and increase confidence in their implementation. More broadly, protecting the integrity of the supply chain should not be viewed solely as a cybersecurity matter. Securing the supply chain also requires attention to quality assurance, product and service safety, counterfeit prevention strategies, technology licensing and export control compliance, and customer trust.

Tables 1 and 2 present a concise summary of the key governmental and corporate obligations and recommendations for implementing them (a more elaborate list is provided at the conclusion of each section). They are the culmination of in-depth research and dialogue with senior government, corporate officials, and policy, legal, and technical experts from around the world. They aim to strike a delicate balance between the fulfillment of legitimate national security requirements and the protection of the digital economy and corporate equities.

TABLE 1

Concise Summary of Governmental and Corporate Obligations to Enhance Supply Chain Integrity

Governments	Corporations
Trust	
Prohibit *systemic* supply chain interventions Limit the scope, scale, and negative consequences of all remaining governmental supply chain interventions	Do no harm—refrain from creating, inserting, or aiding the development of systemic vulnerabilities Apply the highest practical level of security and integrity in products and services throughout their life cycles to prevent abuse, misuse, and undue exploitation
Accountability	
Establish internal processes and consultative mechanisms to make informed, risk-based decisions regarding supply chain interventions and vulnerabilities	Quickly address known vulnerabilities and abuse of products, features, data, and communications
Pair supply chain interventions with a comprehensive plan for mitigating the adverse consequences if exposed	Consistently assess the implications of quality and safety concerns for their broader supply chain integrity ramifications
Implement an efficient process to notify affected entities of detected vulnerabilities	Same
Refrain from denying or significantly degrading the ability of corporations to lend support, and provide updates, and upgrades to existing customers	
Transparency	
Publish policies and procedures for handling supply chain security and vulnerability concerns	Make public the core principles and practices governing the security of products and services
Lay out clear and transparent criteria for the accreditation of ICT/OT vendors and certification of their products and services, and include provisions for mutual and reciprocal certification and accreditation	Make products and services available for reasonable scrutiny by prospective and actual customers and competent governmental authorities Inform current and prospective foreign customers of any directions from suppliers' home governments that conflict with those of the foreign customers' governments or could undermine suppliers' ability to honor their contractual obligations or contradict the laws of the customers' governments
Receptivity	
Establish channels with corporations and pertinent stakeholders, including other governments to discuss issues pertaining to supply chain integrity	Respond expeditiously to lawful and reasonable law enforcement and national security concerns and requests for available information

TABLE 2

Concise Summary of Potential Mechanisms for Effective Implementation and Next Steps

Governments	Corporations
Platforms for Anchoring the Obligations	
Unilateral or collective declarations by governments and/or corporations pledging to honor and promote these obligations Formal bilateral and multinational trade arrangements and/or less binding other international documents (by the G7/G20 communiques, GGE, OEWG, WTO, ITU, OECD)	Technical standards-setting organizations, both domestic (for example, NIST) and international (for example, ISO, IEC) Corporate-led processes (for example, Tech Accord, CoT) or multi-stakeholder processes (for example, OECD Global Forum) Dedicated CSR/ESG initiative that promotes high security and supply chain integrity standards
Additional Incentives for Adherence	
Deny outliers access to government contracts or national markets Introduce mutual accreditation and certification mechanisms for approved vendors, products, and services	Create reputational benefits for adherence and compliance Harness private sector mechanisms, including due diligence procedures of key stakeholders, to encourage compliance
Mechanisms for Verifying Compliance	
Leverage best practices for enhancing performance, safety, and quality assurance (for example, certification of suppliers and subcontractors, audits, chain of custody, traceability, root-cause analysis) to aid investigation of discovered vulnerabilities	Invite governments to support and expeditiously inform private sector analysis of vulnerabilities and, as practical, also their origins. Establish an independent, international mechanism to *technically* analyze and diagnose discovered vulnerabilities
Next Steps	
Outreach and briefings to individual governments and corporations to seek buy-in for core principles and encourage pledges to honor them Engage with private sector stakeholders to develop further incentives	Initiate a process to develop mechanisms and techniques for the verification and operationalization of standards Explore options for launching a CSR/ESG initiative

Introduction

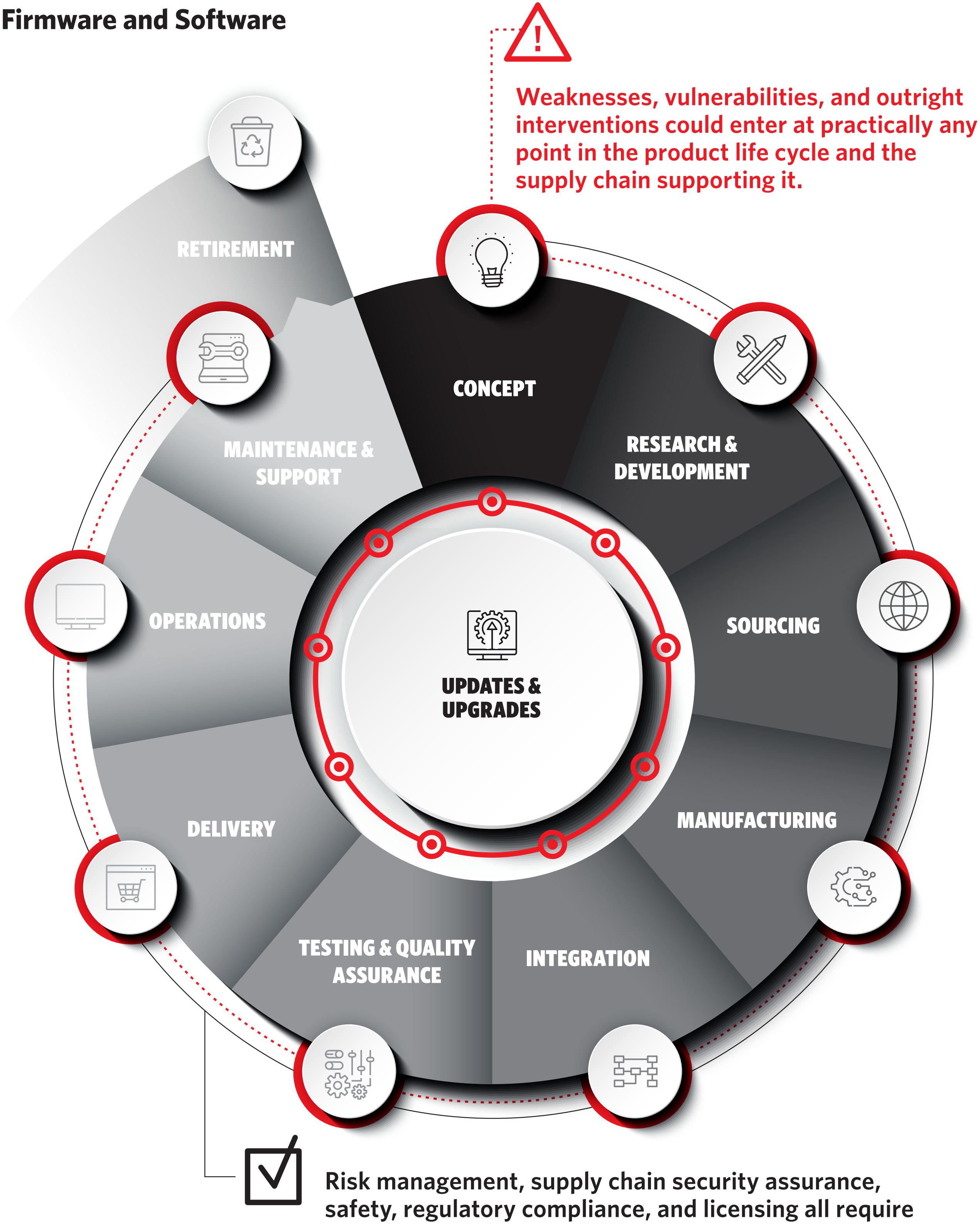
Reliable information and communication technology / operational technology (ICT/OT) products and services are now an indispensable part of modern life at the local, national, and international levels.[1] But much of their performance hinges on efficient and secure supply chains that have minimal inadvertent flaws or vulnerabilities and that guard against harmful interventions. Both natural vulnerabilities and intentional manipulations and other interventions by state and nonstate actors (driven by legitimate if perhaps myopic intentions, as well as nefarious ones) can lead to unwelcome and unintentional consequences. These consequences may include breaches in confidentiality of data, disruption of operations and corruption of data, and violation of the integrity of the algorithms for processing it. In some cases, physical damage to property and people can also result. The harmful effects can extend well beyond individual business enterprises, shareholders, employees, customers, and host nations. The exposure of potentially millions of systems to malicious attacks by the Meltdown and Spectre vulnerabilities discovered in ubiquitous Intel and AMD chips, which remain widely vulnerable to attack because the long available fixes have only been patched by a small percentage of their users, demonstrates how widespread the consequences of flaws in core ICT supplies can be.[2] The health of cyberspace, the openness of the international digital economy and trading system, and the stability of major power relations depend on confidence in the integrity of ICT/OT supplies.

Threats to the supply chain exist throughout the life cycle of products and services, from the gathering of source materials and development of components—including hardware, software, data, and algorithms—to the modifications and upgrades by and for customers (see figure 1).[3] Most concerning is that decisions made in the development phase can affect vendors' ability to manage vulnerabilities and the consequences of interventions. Manipulations early on in the supply chain could have a multiplier or domino effect. Other global industries have faced somewhat similar challenges, perhaps most notably the pharmaceutical industry's defense against fake products (see Appendix 1). But the longer operational phase of the ICT/OT life cycle poses innumerable additional challenges to sustaining the integrity of the supply chain.

Commonly known interventions by governments or corporations include consciously undermining broad security measures, such as encryption standards,[4] and categories of, or widely available products; inserting backdoors or other remote access capabilities into products; or otherwise building undisclosed features and functions into them. To date, these interventions have not fundamentally affected global reliance on ICT/OT. But revelations of systematic intervention or other serious forms of tampering in the supply chain (such as counterfeiting components and products) are already shaking governments' and users' perceptions of the integrity of ICT/OT products, services, and vendors. There is rising concern that manipulations could have destabilizing consequences for the global economy and geopolitical relationships (see box 1).

FIGURE 1

ICT Supply Chain Life Cycle for Firmware and Software



Weaknesses, vulnerabilities, and outright interventions could enter at practically any point in the product life cycle and the supply chain supporting it.

Risk management, supply chain security assurance, safety, regulatory compliance, and licensing all require a synergetic approach toward quality assurance and end-to-end discipline, traceability, and visibility.

BOX 1

Destabilizing Consequences of Supply Chain Interventions

Lost confidence: Trust in ICT/OT products and services that support essential government and commercial systems and applications is widely undermined. This could accelerate balkanization (see below) of the ICT/OT marketplace and undermine confidence in the digital ecosystem itself.

Unintended/collateral impacts: Interventions in standard products and services used globally—especially for military and civilian control systems—may well have diverse cascading effects. These range from creating legitimacy for other actors to engage in similar action; spreading direct effects via self-propagating and/or replicating features, such as viruses (which could be difficult to contain); and proliferation of malicious capabilities, some of which could be reverse-engineered and misused by other actors.

Escalating competition: Discovery of deliberate interventions causes lead state actors to compete and seek new tools and techniques to undermine each other's supply chains. More widespread use of these tools and techniques, including by criminals, could magnify the first two consequences above.

Reputational costs: Publicly exposed government interventions damage commercial brands and interests. This could hurt the broader "brand" value of a country's ICT/OT products and may accelerate the favoring of one country's products over another or over global ICT companies.

Balkanization: Anxieties over interventions and systemic disruptions in the supply chain, especially for global products and services, lead governments to rely on indigenous vendors and service providers. ICT markets and supply chains become increasingly divided along national or alliance lines. This could have a significant negative impact on innovation, competition, and openness in the global economy.

Politicization: Widely suspected or discovered interventions become major political events that further undermine trade and impede cooperative processes to resolve disputes and restore trust.

But deliberately stoking or exaggerating anxieties about supply chain integrity—for strategic, commercial, or political purposes—may produce similarly undesirable effects and be counterproductive. At a minimum, trust in ICT/OT and relationships could be further eroded.[5] Consider how the Huawei case is unfolding. Regardless of the validity of U.S. suspicions that Huawei's 5G equipment could serve the interests of the Chinese government, the highly publicized allegations and ensuing ban on procurement of Huawei products (and massive pressure on others to do the same) alongside severe tightening of component supply for their products are already having profound effects on both national and corporate decisions and relationships. Beyond the effects on costs and availability of products and services, these actions are exacerbating general trade tensions between the United States and China, clouding U.S. relationships with some of its allies that do not fully share its concerns, affecting corporate decisions like whom to buy from and sell to, and where to locate production. Relatedly, these actions are accelerating Huawei and other Chinese firms' quests for self-sufficiency. Even more profound consequences for security relationships (such as U.S. intelligence sharing arrangements with some of its closest allies) and the global economy (innovation and productivity) seem in store.

Despite the risks, the reality is that certain states, some corporations, and others have and will continue to use supply chain interventions to advance their national security, law enforcement, commercial, or criminal interests. In their efforts to counter weapons proliferation, terrorism, subversion, and influence operations as well as other threats, governments may intervene to gather domestic and foreign intelligence, conduct covert operations, and facilitate potential military operations, including through creating physical or cognitive effects. They might even purposely undermine trust in other countries' products and services. There are already reports that the U.S., Chinese, and Russian governments, or entities widely suspected doing their bidding, have enacted or are contemplating several highly secretive operations.

All three countries have been accused of efforts to manipulate their own or each other's supply chains. Particularly notable are U.S. claims alleging a vast Chinese effort to insert compromised motherboards into U.S. supply chains.[6] Western intelligence agencies have blacklisted Lenovo computers due to suspicions that backdoors were giving the Chinese government access to data.[7] The U.S. intelligence community has alleged that Russian actors compromised the product supply chains of at least three industrial control system vendors (that run critical U.S. infrastructure) to distribute malware via legitimate software updates.[8] Meanwhile, classified documents leaked by Edward Snowden have been used to accuse the U.S. National Security Agency of compromising encryption used by security vendors and inserting backdoors into products.[9]

Although typically carried out in secrecy, state actors view their operations as legitimate. Explicit legislation in several countries provides a legal basis for states to engage in such action.[10] China's

Cybersecurity Law, 2017, requires companies to provide "technical support" to national security and law enforcement investigations and to subject their products to governmental security reviews. Russia's recent anti-terrorism law, 2017, similarly requires companies to provide decryption keys to the Federal Security Service to give them access to communications. Australia's 2018 amendment to its telecommunications law has been widely interpreted to give the government authority to force companies to provide backdoor access to encrypted communications.

It is practically impossible to assess the scope of state interventions given the numerous ongoing revelations and allegations. This is due to the secrecy and compartmentation surrounding such operations and how difficult they are to detect. Interventions may also be technically indistinguishable from vulnerabilities deliberately or inadvertently introduced by producers. Vendors are increasingly building remote access mechanisms into their products for various purposes, including gathering information on product usage, conducting maintenance, implementing upgrades, and extending service contracts to enhance revenue. However, such features could be hijacked by malicious actors to target vendors' customers, or even abused by corporations themselves for unsavory purposes (such as to illicitly collect information on their customers). Moreover, governments might persuade or compel corporations to allow them to exploit these features. Even sophisticated corporations might be inadvertently opening the door due to delivering products with inherent, unacknowledged (or undetected) security weaknesses and vulnerabilities (see box 2).

Although uncertainty about the scope and origin of interventions will likely persist, increased awareness of the potential consequences is generating some favorable dynamics. Technology developers and suppliers, buyers, governments, and nongovernmental organizations are undertaking various initiatives to prevent and manage supply chain problems through both unilateral and collaborative efforts. Most of these initiatives focus on requirements, standards, and guidelines to enhance supply chain integrity, as laid out in sophisticated supply chain risk management practices.[11] Other initiatives, mostly in Europe, focus on elaborate processes for certifying products and vendors. For instance, the European Union (EU) Agency for Network and Information Security is helping to develop a common EU-wide certification framework for ICT products.[12] At the national level, the French Network and Information Security Agency already has a process for evaluating and certifying the security of ICT products.[13] Meanwhile, the U.S. Department of Homeland Security leads an ICT Supply Chain Risk Management Task Force launched in 2018 to facilitate public-private cooperation on managing cyber threats to the global ICT supply chain.[14]

But while these efforts are beneficial, they heighten concerns about the broad balkanization of the supply chain and focus mainly on the management of risks associated with accidental flaws or vulnerabilities in hardware and software. No similar, comprehensive effort has thus far tackled *deliberate* interventions by states and corporations—a deficiency that will become more problematic in the coming years. There are at least seven clear reasons why governmental supply chain manipulations will remain, or become increasingly, attractive:[15]

1. They can generate larger troves of intelligence on targets of interests, without having to conduct risky espionage operations or have an on-the-ground presence.
2. Innovations like 5G technology, 3D printing, machine learning, and other data-driven processes as well as new governance structures (such as smart cities and grids) both greatly increase the attack surface for interventions (for example, through adversarial learning) and expand the scope of potential consequences.
3. They could produce other useful and sometimes unique effects—for example, to degrade performance in the context of covert actions, most notably both for counterproliferation (such as Stuxnet) or counterterrorism (such as in the fight against the self-proclaimed Islamic State).
4. Platforms can be created to set a time for initiating desirable military operations (for example, against critical infrastructure or nuclear assets) in the course of armed campaigns, especially in the early phases of warfare or gray zone confrontations.
5. There can be a significant time lag between interventions and effects, between embedding a platform for future attack and the ability to reap the benefits of such operations. But the time and effort required to establish well-placed bridgeheads and the uncertainty of success creates a strong incentive to insert such capabilities well in advance of their utilization, even in the absence of a decision to trigger their effects.
6. Extreme secrecy and compartmentation increase the lure of such operations (and the ability to minimize some of the attendant risks of carrying them out).
7. Strategic and commercial competitors may seek advantage in hyping and politicizing legitimate supply chain concerns, even if this could further erode trust in the integrity of the ICT/OT supply chain.

These incentives—as well as inevitable flaws in hardware and software—mean that supply chain interventions will persist and total trust in the integrity of products and services will not be achieved. But given the potential destabilizing consequences that supply chain untrustworthiness could impose on national and global economies, governments and corporations have objective interests in taking complementary steps to enhance supply chain integrity and mitigate the adverse impacts of manipulations. As they do so, they will need to answer a central question: What is the proper balance between the desire of governmental agencies to compromise, and take advantage of, supply chains vulnerabilities in the interest of national security and the desire of practically everyone else to enjoy trustworthy ICT/OT products and services?

BOX 2

Acute Threats to the Integrity of the ICT Supply Chain

Compromised software vendors: Between 2013 and 2014, a hacking group dubbed Dragonfly by Symantec is alleged to have compromised three European vendors of industrial control systems, leading to hundreds of users installing "Trojanized" software.[16]

Preinstalled undisclosed features: In 2015, hundreds of thousands of Lenovo computers were reportedly discovered to have hidden, preinstalled third-party "adware" that allowed access to users' sensitive personal information and compromised browser security.[17]

Hijacked update mechanisms: In 2017, the update mechanism for a piece of Ukrainian accounting software used by many multinational corporations operating in Ukraine was compromised, allowing the NotPetya cyber attack to rapidly spread around the world, causing massive disruption and as much as $10 billion in total damages, according to a White House estimate.[18]

Systemic vulnerabilities: In 2018, the discovery of Meltdown and Spectre revealed what security researchers describe as a new class of fundamental security vulnerabilities affecting chips almost universally relied upon around the world in everything from cell phones to servers.[19]

Critical service providers hacked: Operation Cloud Hopper, a major hacking campaign stretching from around 2014 to 2018, reportedly compromised some of the largest global cloud service providers to steal information from their clients.[20]

Note: These are just a handful of high-profile examples to illustrate the scope and magnitude of the challenge and its different permutations and by no means represent an exhaustive list.[21]

To help move the discussion forward, this paper proposes obligations that governments and corporations should undertake to prevent, manage, and redress interventions as well as diminish weaknesses and vulnerabilities that place the integrity of ICT/OT supply chains at serious risk. It also offers ways to encourage governments and corporations to adhere to these obligations, as well as measures to discourage all others from impeding them. The proposed obligations are divided into four mutually reinforcing categories: trust, accountability, transparency, and receptivity. Taken together they constitute a normative framework that governments and corporations could adopt, effectively binding themselves to do no harm to the ICT/OT supply chain. Broad adherence to them will go a long way toward rebuilding confidence in the integrity of this supply chain.

These obligations, and the ways to anchor them and incentivize and verify compliance with them, are the culmination of extensive interviews with current and former senior government officials and the legal and security officers of leading ICT vendors in multiple countries, including the United States, Europe, China, and Israel.

The research was originally designed to focus solely on government manipulations of ICT/OT products and services, but the government officials interviewed indicated that curtailing the manipulation of products and services would be more feasible if corporations adopted corresponding obligations that enabled states to meet legitimate national security and law enforcement responsibilities. In turn, the legal and security officers interviewed highlighted the need for incentives that would reward those who abide by the obligations and penalize those who do not. The central concerns then became how to verify that the commitments are being fulfilled, how to assess and attribute allegations of supply chain manipulations, and who should do it. In sum, the obligations, incentives, and verification arrangements proposed in this paper grew organically from many iterative engagements with leading technical and policy experts from government and industry. The result is a rather complicated, nuanced package of proposals. While a simpler package would be desirable in many ways, it would not realistically meet the core needs of the various stakeholders.

Substantive Governmental Obligations

In carrying out any intervention, states have a major responsibility—to minimize harm to the ICT/OT supply chain. This could be fulfilled by either refraining from conducting systemic interventions in the supply chain or at least minimizing the negative consequences of interventions by narrowing their scope and building safeguards into them. Such policies and actions would complement policies and requirements that states already pursue to enhance their own procurement processes or to inspire others to follow.

Refrain From Systemic Interventions

One major commitment governments can undertake to enhance trust in the integrity of ICT/OT products and services is to refrain from introducing systemic interventions in the supply chain. There is a key distinction between discrete and systemic interventions. A discrete intervention, such as placing an implant in a single piece of industrial control software destined for a specific target, could meet a significant national security need and have a relatively limited and predictable effect. Whereas a systemic intervention affecting all "copies" of a type of hardware or software or in an entire series, version, model, or production line, could have far wider and much more serious implications. There are gray areas, of course, such as when interventions affect *all* copies of a product that is intentionally offered only to a limited clientele or when interventions affect a limited production run destined for one customer or customer state.

The commitment of even a few governments that would otherwise have the motivation and ability to carry out systemic interventions would make a real difference. Their agreement would go a long way toward addressing customer and vendor concerns and, in turn, make the opposing position of other governments increasingly less tenable. It would be relatively easy to verify compliance by demonstrating that an intervention is not systemic. The legitimate space for interventions would gradually be scaled back to discrete cases[22] involving certain products that governments strongly suspect are being destined for, in route to, or already possessed by the "wrong hands."[23]

Eschewing systemic interventions while allowing discrete ones could strike a welcome balance. National security interests could still be pursued through discrete interventions, while refraining from systemic ones would serve the commercial and public interests in uncompromised systems.[24] In a world with so many unintentional vulnerabilities and other attack surfaces, governments have little need to create new ones. Many governments have existing legal arrangements for information sharing that allow them to acquire similar kinds of intelligence without having to compromise products. These could be refined to meet both the intelligence needs of governments and the transparency needs of corporations. Furthermore, regarding the parameters of discrete interventions, current legal information-sharing arrangements between corporations and governments already abound. They could be further refined, working out appropriate modalities and mechanisms for making such intervention requests acceptably transparent.[25]

One issue to consider, however, is the possible distinction between interventions in the domestic and international supply chains. Some governments may consider it essential and reasonable to intervene in their own domestic supply chain. These governments may legally (or otherwise) compel suppliers and service providers operating in their sovereign domain to cooperate, as they do, for example, in requiring them to reveal source code or retain data. This obviously diminishes overall trust in their supply chain and makes it especially difficult for compliant corporations to expand into the international marketplace. However, even in these cases, it would be worth securing the government and corporations' commitment to refraining from systemic interventions when operating internationally. Competitors will make a significant effort to verify adherence to these commitments.

Introduce Safeguards

Regardless of whether states refrain from using systemic interventions, the international system would greatly benefit from establishing operational and technical safeguards to minimize the adverse, unintended effects of interventions. Operational measures could include refraining from interventions in products designed for sensitive sectors or applications (for example, software or hardware intended for medical applications). States could also renounce, or at least severely restrict, interventions in operational technologies that support critical infrastructure (for example, nuclear power plants, and water supply systems) or disrupt and degrade financial transaction.

Ideally interventions should not be designed to introduce self-replicating, self-propagating, or deep persistency features into ICT products and systems.[26] Such features can help overcome network defenses, making them attractive for intelligence collection and covert operations, but their ability to replicate or spread can have significant unintended consequences, including enabling adversaries to reverse engineer them. These consequences, in turn, threaten the reputation and brand value of all the companies affected.

If states refuse to rule out self-propagating, self-replicating, and deep persistency features because of their intelligence appeal, they should at least commit to build in safeguards that seriously constrain and mitigate their adverse effects. Very specific targeting parameters could ensure that any malware intended to alter the performance of a system could only be triggered by precisely defined circumstances in the target environment. For instance, the Stuxnet worm that targeted Iran's nuclear centrifuges only deployed its payload against a specific line of Siemens programmable logic controllers (PLC) in the precise configuration used in Iranian facilities.[27] Thus, even as it unintentionally and unexpectedly spread to tens of thousands of computers around the world (likely including others with the same industrial control systems) Stuxnet did not damage them because of certain ad hoc safeguards that were purposefully built into the malware.[28]

Another safeguard could be a built-in "expiration date" for the intervention's effects. Stuxnet, for example, was programmed to stop replicating after June 24, 2012. Other feasible safeguards include a kill switch (to immediately terminate its adverse effects) as well as the development of a parallel ready-to-introduce fix that could quickly eliminate the vulnerability being exploited. This could also enable the intervention to be terminated, withdrawn, or patched once its utility expires or when the consequences of its introduction prove to be excessive.

Procedural Governmental Obligations

A second approach to minimizing harm to the ICT/OT supply chain could be *procedural* and apply to both systemic and discrete interventions.

Assess the Risks and Require Approval

To enhance trust and accountability, supply chain interventions could require senior-level approval. Before an approval could be granted, however, a competent authority would need to (1) assess the likely security and economic consequences and potential collateral damage and (2) ensure that safeguards have been built into the operation. This process would be analogous to the U.S. Vulnerabilities Equities Process, which determines whether and when vulnerabilities discovered in products are disclosed to vendors for patching or reserved for exploitation to conduct cyber operations.[29] In every government where such supply chain interventions are contemplated, they should be subject to an interagency review body that similarly weighs both national security and economic perspectives. Such a process is both critical and viable even among states that are reluctant to formally set up, let alone publicly admit, they have in place a review process of this nature.

Inherent uncertainties surround the effects of any intervention and make it difficult to accurately predict the potential consequences. Some form of quasi-judicial review and/or generic parliamentary oversight would help ensure at least consideration of diverse perspectives and equities. Naturally, all parts of the process would have to meet secrecy and compartmentation requirements; any external oversight mechanism would have to be largely confined to verifying that the interventions comply with the relevant policy guidelines and that the assessment of the interventions has been carried out methodically and consistently.

Regardless of the specific procedures governments establish to review and approve interventions, they must assess the potential broad consequences from the micro to macro level—including implications not merely to the affected consumers and the specific corporate brands and their employees and shareholders involved, but also for national reputation, and even the functioning of the international trade and security systems. The key question would be, “What are the consequences if the interventions lead potential customers to believe that the country’s and companies’ products are compromised and worse still, exploited for surveillance or other purposes?” Notably, states could more easily address this concern if they have renounced using systemic interventions. If discrete interventions were discovered, it would be relatively straightforward to verify that all or at least most other “copies” of the hardware or software had not been similarly corrupted.

It will also be important to assess (1) the level of confidence the perpetrators have that the intervention’s damage would be proportionate to the objective sought, (2) the intervention’s duration and scope (whether it is temporary and/or reversible and localized), and (3) the risk of tools and techniques being exposed, reverse engineered, or repurposed. The global WannaCry and NotPetya attacks were enabled in part by an exploit reputedly developed by the U.S. National Security Agency (NSA) and leaked by a hacker group called the Shadow Brokers, demonstrating the risks inherent in creating cyber tools even in the most closely guarded context. Such tools can be even more worrisomely employed through software update mechanisms.[30]

Additionally, governments should conduct follow-up, periodic assessments to evaluate the benefits, risks, and other consequences of sustaining the action, particularly in light of the original requirements, evolving circumstances, and accumulated effects. Explicit approval should be required for any extension or expansion of an intervention. Finally, a comprehensive plan should be in place to mitigate an intervention's adverse consequences if it is exposed or proven highly detrimental to corporate, national, and/or international interests.

Distinguish Between Intelligence-Gathering and Covert (and Military) Operations

In general, actions that violate the confidentiality of information are less destabilizing than those that affect the actual performance of systems. In general, merely encroaching on the confidentiality or even availability of systems would probably not trigger the immediate anxiety and prospects of retaliation that qualitative substantive manipulations would produce. This holds especially true if the interventions are undertaken clandestinely and carried out in a targeted fashion. In contrast, manipulating systems' performance—for example, to produce operational military effects such as causing weapons to malfunction—poses far greater risks for triggering uncontrolled and unintended consequences than those associated with extracting data for intelligence purposes. Similarly, significant difference exists between the potential adverse effects inherent in denying access and availability of systems, compared with manipulating data integrity and the algorithms that process and control its employment in various systems. Granted, some of the distinctions here are a matter of nuance, as even the loss of availability of ICT services could affect the integrity of a service (for example, if financial market trades were delayed by even a fraction of a second). But the general principle still applies.

These considerations lead to another procedural recommendation. Namely, the approval process proposed above should recognize the distinctions between different types of interventions into the supply chain. Far greater care and stricter criteria should be exercised when considering interventions that have such potential to cause loss of trust and trigger physical effects, certainly in peacetime and especially in dual use (as distinguished from pure military) assets such as ICT/OT systems. It is vital for governments not to underestimate the potential blowback that would ensue not only when these operations trigger their intended effects but also when such activities are discovered or even widely believed to occur.[31] Consequently, if they cannot forswear such practices entirely in situations short of war, they should use them sparingly, especially against assets that serve civilian as well as military functions. Moreover, prudence would require that any proposed operation manipulating systems, algorithms, and data integrity require elaborate senior-level interagency and inclusive consideration of its potential effects.

Consult With Corporations

Approval of an intervention could also require private consultations with vendors to secure their informal consent to, or at least acceptance of, intrusions into their ICT/OT products and services. The benefits for both governments and corporations are self-evident. Governments could potentially minimize conflicts with the corporations and gain some invaluable technical and operational knowledge. Such consultations may not enhance overall trust in the supply chain or in the brand name/product, but they could help mitigate the adverse effects of interventions. Corporations could sensitize governments to some of the risks involved, as well as work out some arrangements to prevent unintended consequences for the individual corporations involved. With a corporation's assistance the risks and unintended consequences of an intervention could be reduced through more precise and reliable targeting—for example, confining interventions to domestic applications (as discussed earlier) and/or ad hoc cases. In high-risk scenarios, corporations could be given a hearing to make their case to the government why such behavior should be constrained or be ruled out.

Although the idea of consultations may be contentious, corporations are not oblivious to the reality that governments have legitimate national security reasons to collect information by leveraging or even creating (in extreme cases) vulnerabilities in the supply chain. Nor can they discount that, in rare cases, governments might need to manipulate products and services for offensive purposes. Some privately held corporations might consider it their patriotic duty to assist governments. Others might cooperate in order to gain some commercial benefit or acquire greater leverage and influence in negotiating the terms of interventions. Governments also typically have multiple tools at their disposal to incentivize and reward corporate collaboration. Some governments may have lawful ways to require cooperation and directly or indirectly penalize noncollaboration.

Therefore, some corporations might actually seek or voluntarily agree to consultations.[32] But the overall risks to the brand name as well as other liabilities posed by interventions will likely make most corporations reluctant to participate in the approval process unless compelled to do so by law. Even then, they may lobby hard against such a process by legally challenging the law in court. And it is highly doubtful that publicly traded corporations would formally negotiate the terms of interventions targeting their own products and services. Hence, an informal process might prove a more viable practice in those cases.

Regardless of what motivates governments to pursue corporate cooperation, how they secure it, and how corporations participate, prudence requires limiting the scope of the cooperation as much as possible and agreeing to its parameters in advance. For example, corporate consent could be given on a case-by-case basis to discourage systemic interventions. Governments (and their employees) could also agree to confidentiality provisions and to restrictions on using knowledge about products or services for subsequent interventions. Other provisions could include repercussions for abusing the agreed-upon terms of an intervention, such as sanctions against former government employees for using information they acquired while in the government service.

In reality, governments can force corporations operating (or wishing to operate) on their soil to comply with their wishes, and they might have legitimate reasons to do so. Yet governments need to consider the consequences of an excessive use of power, especially when interventions might affect other countries. The consequences of aggressive interventions go beyond the immediate vulnerabilities they create. States must weigh not just the potential for direct harm but the risks of normalizing such risky behavior, which in turn could be used by others against their societies' broader interests.

In this context it is also essential to raise the issue of governmental interventions that deny or significantly degrade the capacity of corporations to honor contractual obligations to existing customers to support, update, and upgrade products they have purchased. Governmentally induced supply disruptions (of raw materials, components, and systems) have become common place in recent years. Whether in the form of governmental sanctions or other administrative actions, these actions make it difficult or impossible for corporations to honor their contractual obligations to their customers. This, in turn, severely undermines the credibility of suppliers operating in certain jurisdictions. Such interventions assume especially grave implications when ICT products and services are involved, as these typically have a huge, global supply chain that undergirds production lines, enables critical infrastructure, facilitates core services, involves massive investments, and has long life cycles. Customers then suffer from doubts about vendor capacity to support such products and services. It is thus reasonable to expect of governments acting in the broad interest in the digital economy to refrain from disrupting such essential corporate services to existing customers and more broadly hold back from creating systemic doubts about the trustworthiness not only of technologies but also of their servicing.

Table 3 summarizes the potential substantive and procedural governmental obligations just described. They are categorized by the broader goals of building trust, accountability, transparency, and receptivity. The first two categories involve substantive governmental commitments to act in a manner that greatly diminishes the prospects of supply chain interventions. The latter two categories complement the former two by adding measures designed to inform and impress all pertinent stakeholders that they are indeed behaving in such manner and are open to dialogue to further enhance confidence in their responsible behavior in this domain.

TABLE 3
Potential Governmental Obligations

Trust

Prohibit systemic supply chain interventions

Limit the scope, scale, and negative consequences of all remaining governmental supply chain interventions:

- Prohibit interventions in certain sensitive areas (for example, the medical sector)
- Introduce operational and technical safeguards in interventions to limit their replication, propagation, and duration and to minimize prospects for the reverse engineering of tools

Accountability

Establish internal processes and consultative mechanisms to make informed, risk-based decisions regarding potential and ongoing supply chain interventions and the handling of vulnerabilities:

- Develop clear internal risk frameworks and criteria for interventions
- Assess both the security and economic risks of supply chain interventions, including the potential impacts on vendors and brands, consumer confidence, and commercial competitiveness
- Establish a high-level authority and process for approving supply chain interventions designed to create covert or military operational effects
- Require the periodic assessment and approval of long-term interventions
- Create a user-friendly mechanism for policymakers to make informed judgments about the risk of detection
- Create a comprehensive plan for mitigating the adverse consequences of an intervention, if exposed
- Consider holding informal consultations with the corporations that may be affected by the intervention, if they are amenable to such dialogue

Refrain from denying or significantly degrading the ability of corporations to support and provide updates and upgrades to existing customers

Transparency

Publish policies or procedures for handling supply chain security and vulnerability concerns:

- Make public a summary of laws and regulations related to supply chain security and the processes governments follow to enhance supply chain integrity
- Establish an efficient process for notifying affected companies of detected vulnerabilities
- Lay out clear and transparent criteria for the accreditation of ICT/OT vendors and certification of their products and services, including provisions for mutual and reciprocal certification and accreditation

Receptivity

Establish channels with corporations and pertinent stakeholders, including other governments, to discuss issues pertaining to supply chain integrity:

- Establish clear processes and channels for dialogue, and publicly designate points of contact

Corresponding Corporate Obligations

Complementary corporate obligations could also protect and enhance the integrity of the ICT/OT supply chain. Their inclusion should be considered necessary for three major reasons. First, vendors of ICT/OT products and related services reside almost exclusively in the commercial sector, and therefore, the prospects of their businesses are partly dependent on the marketplace's trust in these products and services. This means that all stakeholders have a stake in encouraging corporations to adopt higher security standards. One group that could benefit the most is corporations operating in states whose governments are willing to renounce or restrict interventions in the ICT/OT supply chain, because these business's products could be deemed most trustworthy. Second, extending commitments to the private sector also would help narrow the room for governments' intentional interventions in the supply chain through corporations and their employees. Finally, private sector commitments could assist in limiting the danger from unintentional vulnerabilities in the supply chain. This is important because the exposure of vulnerabilities—by accident or malevolence—could have equally destabilizing consequences in an age when ICT/OT products and services are supporting vital infrastructure and services around the world.

Some corporations are already working to enhance trust in their wares. Most are doing so unilaterally, such as Intel's impressive broad-based computer life-cycle assurance initiative, but industry-wide initiatives—such as Microsoft's Tech Accord, Siemens' Charter of Trust, and the Open Group Trusted Technology Forum—have recently emerged.[33] To date, these initiatives, while laudable, remain limited. None encompasses all of the relevant global stakeholders or comes even close to addressing the full range of issues relating to ICT supply chain integrity. Hence, there is a need to augment existing efforts with a more comprehensive, globally oriented set of principles that corporations could be encouraged to adopt. Such cooperation could counteract the increasingly toxic politicization of the debate surrounding the integrity of the supply chain.

Some may argue that the proposed corporate obligations below are too ambitious. Yet they build on many widely acknowledged, vital elements of trust that leading companies are already pursuing piecemeal. The same steps to ensure supply chain integrity also serve to enhance product safety, performance (quality assurance), licensing arrangements, export control compliance, and marketing (customer trust). The synergies between these corporate interests and practices thus provide a compelling rationale for undertaking these obligations in any event. Moreover, there are commercial advantages associated with diminishing the risks of compromised or counterfeit components and systems entering the supply chain or displacing it.

Do Not Support Systemic Interventions

To build confidence in both customers and governments it thus seems reasonable to expect all corporations to similarly subscribe to the basic norm to *do no harm*, and operationalize this commitment in the same four complementary areas:

- Trust in product/service life cycle (R&D, production, service)
- Accountability
- Transparency
- Receptivity (to lawful and reasonable law enforcement and national security concerns)

To maintain trust in the supply chain, corporations should categorically refuse to create or aid the development of *systemic* vulnerabilities in their products and services (for any purpose).[34] Further, they should ensure that their employees and subcontractors commit to the same obligation, so the entire supply chain is protected.[35]

Protect Products and Services Throughout Their Life Cycles

Additionally, corporations should undertake certain practices (described below) for the secure development of their products and services and the proactive management and mitigation of weaknesses and vulnerabilities throughout their life cycles. These practices can build on existing and evolving standards and frameworks, including those of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) ISO 27001 (formally known as ISO/IEC 27001), which specifies an information security management system (ISMS); IEC 62443 (formerly known as ISA 99), which is the global standard for the security of industrial control system (ICS) networks; and the Secure Development Principles (anchored in ISO/IEC 27034 standard) right from the design stage.[36] The latest version of ISO/IEC 15288 system engineering standard for all types of systems embodies an even more daunting standard, although this realistically might be difficult to apply commercially across the board.[37]

Most importantly, corporations should protect against the misuse of features like remote access and update mechanisms that constitute prime attack vectors. It is difficult to overstate the importance of this obligation. Companies now routinely use such features to maintain, upgrade, and patch systems quickly without a significant burden on users, as well as to gain valuable commercial and technical information on product usage. These features provide enormous value for both companies and consumers, but they can also be misused. Consumer trust in these features is vital. Major incidents like those involving Kaspersky Lab and CCleaner are degrading that trust.[38] Thus, corporations—and subcontractors providing components, products, and services—need to commit to high standards of security in the design and management of these kinds of features.[39] They also should help customers fully understand the remote access mechanisms, their purpose, and how they are utilized. Customers should have the ability to turn off the mechanisms without disabling the performance of the entire product. Accompanying transparency measures should reassure customers that there are no undisclosed remote access features, and that acknowledged ones will be used solely for purposes that customers agree to. Customers are entitled to expect vendors to provide them with both comprehensive transparency and assurance of products' integrity for their entire life cycles.

The need for vendors to attend to the security of products they sell throughout their life cycle is particularly important and challenging. Challenging not least because the necessary level of post-sale security support entails effort and cost and also could be seen to adversely affect demand for newer products and services that such vendors may offer. Yet, weaknesses and even outright vulnerabilities in products often surface (and in some cases are even introduced through subsequent upgrades and modifications) quite a while after products have been acquired, making vendor commitment to attend to them critical, especially as some products or at least legacy components thereof have long functional lives. At a minimum, vendors must convey to customers understandings of the period for which they would be eligible for security support.

Handle Discovered Vulnerabilities Quickly

When corporations discover or are informed of vulnerabilities in their products and services, they need to expeditiously notify their customers, resolve the problem, engage in root cause analysis, and address the source. Corporations could establish vulnerability disclosure policies and engage in other practices that would bring to their attention vulnerabilities discovered in their products and services and suggest how to disclose and address them.[40] Insights gleaned from discovered vulnerabilities should feedback into a process of continuous improvement. Root cause analysis of major vulnerabilities allows the developer or service provider to prevent future products from being undermined in the same manner. Further, sharing these insights with others in the industry would help raise the security standards of all ICT/OT products and services.[41]

Protect Customer Information

ICT/OT vendors need to respect and protect the customer information they collect and use. Two separate challenging issues arise here. First, what are the parameters for handling this information? Second, what information can they share with governments and under what conditions?

Corporations should subscribe to clear, transparent, and rigid rules on the permissible use of information gathered about customers and their use of products and services. Three essential requirements come to mind. The information corporations gather should (1) align with the scope and purpose defined (in very clear language) in the customers' end-user license agreements, (2) be transmitted securely via encryption, and (3) be stored and disseminated anonymously whenever possible, and when impossible done with equivalent safeguards in place.

Accommodate Reasonable, Lawful Requests for Information

Corporations should also be receptive to legitimate law enforcement and national security concerns and requests for available information. A salutary balance needs to be established between legitimate national security needs and the broader interests of national and international society, including economic well-being. Key governments might be more apt to refrain from intervening in the ICT/OT supply chain if they are confident they have other reasonable means of acquiring the information necessary to protect citizens from criminal and national security threats and can occasionally engage in broader manipulation.[42] Both corporations and governments must act in good faith to find the least destabilizing—and most commercially palatable—way to acquire critical information needed for legitimate and lawful purposes.[43] Some goodwill from corporations could help move wavering governments toward supporting norms of restraint, such as those proposed earlier in this paper.

Possible parameters, modalities, and implications of government-corporate quid pro quos, if any, may not be generic. In any case, this is a bigger challenge than can be addressed here. Generally, corporations could be expected to respond to lawful requests for information if they already possess the information and it was acquired in the state where they operate. In turn, states should consider the potential for immediate harm to the assisting corporation and the precedents that might be created. Some requests could set "legitimate" precedents that would make it more difficult for corporations to resist similar requests from other governments. Finally, it would be prudent to work out mutually acceptable modalities whereby corporations would be able to publicly acknowledge in some fashion lawful requests for access that competent governments make of them.

Most of the above obligations seem straightforward, but they will not necessarily be easy to meet. They are deliberately generic so as not to discriminate among vendors or products based on their country of origin so to allow corporations (with different products and services) some flexibility to work out their preferred methods for meeting the obligations and for evaluating the results. Which naturally brings up the question whether the proposed obligations ought to be codified as standards. There are obvious advantages to setting up (generic) standards. Several of the proposed obligations indeed seem mature enough to operationalize into standards, including by leveraging the existing, widely respected technical standards referenced above. Others may not presently lend themselves to such operationalization but could be developed and codified into standards as they mature. Still others may not lend themselves to codification as generic, technical standards at all and may need to be flexible to adapt to specific circumstances. Some of this last category would thus have to remain inherently high-level obligations that are tested against cases of concrete behavior. A comprehensive list of this nature (which could obviously be further refined and expanded) will hopefully serve as a benchmark against which corporate obligations toward the integrity of the ICT/OT supply chain could be assessed.

There is a clear synergy between several of the proposed corporate obligations. For example, renouncing intentional interventions in the supply chain that customers have not explicitly agreed to and/or that do not serve legitimate purposes aligns with existing high security standards for ICT/OT products and services. The same is true for the corporate obligation to address unintended vulnerabilities expeditiously and globally once they are discovered. Obviously, none of the obligations alone will protect products entirely from unintended vulnerabilities. Yet in combination, they will impose far more stringent requirements on corporations operating in the highly sensitive ICT/OT sector than is the case for corporations handling Internet of Things devices.

As with the government obligations discussed above, the proposed corporate obligations pertaining to trust and accountability are accompanied by additional obligations pertaining to transparency and receptivity. Once again, the transparency obligations suggested below are deemed essential in order to build and maintain the confidence of both governments and customers throughout the world that the corporations are indeed impartially abiding by their trust and accountability obligations. Adoption of such obligations would likely encourage (pressure) other vendors operating globally in this sector to do the same. Introducing reciprocal corporate obligations is also designed to serve another, truly indispensable role: to secure government buy-in. If governments lack confidence that they can enjoy adequate collaboration from corporations operating on their territory to legally obtain all information they reasonably require for both law enforcement and national security purposes, it is hard to envisage them adopting substantive and procedural restraints on their potential supply chain interventions.

Similarly, corporations that market or aspire to market their ICT/OT products and services abroad must consider the possibility that their home government would require them to provide access and/or information, or alternatively, could degrade their ability to provide certain customers with support, updates, and upgrades to their products and services. Such governmental interventions could be undertaken through judicial or extrajudicial processes. Either way, corporate suppliers' would then find it more difficult to assure foreign customers and governments that they (the suppliers) are trustworthy. Corporations could mitigate such concerns at least somewhat by committing to inform their customers if and when the suppliers' home government's guidance might undermine their ability to honor their contractual obligations or contradict the laws of the customers' governments.[44]

Table 4 summarizes the proposed corporate obligations just described. Like the government obligations, they are categorized by the broad goals of building trust, accountability, transparency, and receptivity.[45]

TABLE 4
Potential Corporate Obligations

Trust

Do no harm—refrain from creating, inserting, or aiding the development of systemic vulnerabilities:

- Refuse to work with any government to systematically weaken the security of products and services

Apply the highest practical level of security and integrity in products and services throughout their life cycles to prevent abuse, misuse, and undue exploitation:

- Develop, build, operate, and maintain products and services at the highest appropriate level of security for their entire life cycle
- Protect against the misuse of features that, among other functions, provide access remotely and update systems
- Take active measures to safeguard the communications network used for and by ICT/OT vendors and protect the security, integrity, confidentiality, and availability of the information that goes through it
- Protect the security and integrity of supply chains

Accountability

Quickly address discovered vulnerabilities and the abuse of products, features, data, and communications:

- Expeditiously address critical vulnerabilities discovered in products and services throughout their life cycle (and engage in robust efforts to discover others)
- Create an efficient process to notify all affected entities of detected vulnerabilities
- Obtain explicit customer consent for the remote access and update mechanisms built into their products and services
- Give customers the ability to turn off all vendor-installed remote access mechanisms
- Engage in root cause analysis of discovered vulnerabilities and use the lessons learned for continuous improvement
- Respect and protect private and confidential customer information and obtain explicit permission from customers to collect and use such information

Transparency

Make public the core principles and practices governing the security of products and services:

- Establish extensive transparency and confidence-building measures to reassure governments and clients about the integrity of products and services
- Provide equal and simultaneous access to vulnerability information for all parties globally
- Notify impacted parties of security breaches in a timely fashion
- Document for customers existing features that enable remote access so they fully understand their purposes and how they are utilized

Make products and services available for reasonable scrutiny by prospective and actual customers and competent governmental authorities:

- Share with customers the detailed specifications of product and service features and their expected behavior to allow the customers to independently detect anomalous behavior
- Provide customers with ways and opportunities to confirm with their own or outside experts that products and services fully conform with the expected behavior
- Make public the requests from law enforcement and national security agencies for customer data

Inform current and prospective foreign customers of any directions from suppliers' home governments that conflict with those of the foreign customers' governments or could undermine suppliers' ability to honor their contractual obligations or contradict the laws of the customers' governments.

Receptivity

Respond expeditiously to lawful and reasonable law enforcement and national security concerns and requests for available information:

- Quickly accommodate lawful and reasonable governmental requests for assistance and information to obviate the need for governments to undertake serious supply chain interventions
- Make a reasonable effort to collaborate with governments and other corporations to jointly enhance the integrity of the ICT/OT supply chain and rebuild trust in products and services

Anchoring the Obligations and Incentivizing Adherence

There are numerous practical ways to make progress toward transforming all, or at least some, of the obligations proposed above into a binding normative framework and to incentivize compliance. The paths forward could involve governmental and intergovernmental action, corporate action, and/or multi-stakeholder action. In any case, anchoring these obligations in formal agreements or at least policy declarations would ideally be accompanied by additional actions to encourage adoption and compliance and to "sanction" those that consciously break pledges to honor them.

Most ambitiously (and contentiously), states could anchor the obligations in international agreements, such as trade accords like the recent United States-Mexico-Canada Agreement (USMCA) on digital trade.[46] Article 19 of the USMCA articulates provisions pertaining to digital trade and specifically calls for a risk-based approach to cybersecurity. It de facto incorporates the five functions of the National Institute of Standards and Technology Cybersecurity Framework, namely identify, protect, detect, respond, and recover. Article 28 of the USMCA pertains to good regulatory trade and related practices and includes provisions to promote regulatory quality not merely through internal deliberations, transparency, and accountability but also by creating a joint Committee on Good Regulatory Practices (the GRP Committee). The latter is designed to encourage regulatory compatibility and regulatory cooperation in order to assist in promoting trade through interstate collaboration.

Building on the USMCA language, additional supply chain benchmarks and obligations could be incorporated into other agreements. For example, states could commit to not tamper (categorically or conditionally) with each other's corporations' products. Or states could commit to accept the mutual certification of ICT/OT vendors (or products). The obligations could be anchored in less formal international documents, such as those typically issued by communiques from G7 or G20 summits, the Organization for Economic Cooperation and Development (OECD), or more global reports of the United Nations' Group of Governmental Experts (GGE) and/or Open-Ended Working Group (OEWG). Additionally, the original formula in the 2015 GGE report could be strengthened and expanded upon if the GGE process is productively revived.[47]

In parallel, pertinent international institutions could incorporate norms against intervening in the integrity of another state's ICT/OT products or services into existing trade rules for intellectual property, perhaps those of the World Trade Organization (WTO), or telecommunications standards, perhaps those of the International Telecommunications Union (ITU). Of course, this would involve a lengthy and contentious process, at best.

A second approach, possibly a fallback, would involve action by individual states. Those states that renounce systemic interventions (proposed here as a priority) could legitimately exclude states and/or companies that refuse to commit to or abide by this obligation from accessing their national markets products and services. They could also invoke national security provisions in trade rules to block other countries' ICT/OT products and services that are believed to be unsafe or manipulated. Of course, such measures would be contentious internationally, in part due to the national security exemptions contemplated here.

A narrower version of this second approach would be to have subscribing governments deny corporations and other states access to government contracts if they fail to adhere to core obligations. Some governments already engage in this practice but they should explicate their criteria. Their decisions to exclude shouldn't be arbitrary or discriminate against certain countries' vendors. This could especially apply to ICT/OT contracts involving critical infrastructure (a definition that would inevitably vary between states). This approach, too, would be somewhat contentious and complicated to negotiate in trade forums.

A third, potentially more powerful, approach would allow for the mutual accreditation and certification of vendors, products, and services. Naturally, such arrangements offer considerable economic benefits and, over the longer term, would only be tenable for those states and vendors in compliance with the obligations articulated earlier. In the short term, this approach has inherent limits, as states are unlikely to see accreditation and certification as sufficient criteria for allowing some foreign vendors, products, and services to qualify for contracts in the most sensitive sectors. Generally, states should minimize the types of sectors and projects for which foreign suppliers are excluded from bidding, which would obviously be easier to accomplish if the principles and accompanying standards raise the requirements bar high enough.

A fourth approach would be to highlight reputational risks and benefits. States and corporations that eschew or violate the most critical obligations could be publicly stigmatized. Conversely, states and corporations that adhere to the obligations could be publicly credited. Publics would benefit either way, as their products and services they might buy would be prima facie less vulnerable to systemic tampering and subjected to higher security standards.

A fifth approach would be to develop a credible, broad, and open corporate social responsibility (CSR) process or an environmental, social, and corporate governance (ESG) process around the obligations proposed. Such a process could be combined with or separate from the technical verification process (discussed next). Regardless, a CSR process would include general discussions about upholding and refining corporate obligations to enhance trust in the supply chain in light of technical developments and insights gained from real-life incidents. Corporations could, in turn, demand that their subcontractors and service providers comply with all of the obligations and deny eligibility for contracts to those who fail this test.[48]

The credibility and influence of such a CSR process would depend on the range and depth of obligations its members take up and the scope of the membership, especially internationally. Membership would have to be inclusive and global to have a chance of overcoming political headwinds. The credibility of a CSR process would also depend on the existence of auditing and grievance-airing mechanisms to assess corporate adherence and examine allegations that corporations failed to uphold the security standards. Useful precedents for CSR processes have included such mechanisms.[49] It is worth noting that a credible CSR process (as distinguished from a mere industry association or lobby group) would have far greater clout in influencing governments to adopt their proposed corresponding ICT/OT obligations.

The utility of a CSR/ESG process could be considerable even if it only included several leading entities in the field. It could set de facto industry standards and best practices that could indirectly affect even those corporations that do not participate or fail to comply. In this context, it seems expedient to explore possible collaboration with the Institute for Supply Management—the oldest and largest supply chain organization in the world. The obligations proposed in this paper could be anchored in its 2016 Principles of Sustainability and Social Responsibility and related training and outreach efforts.[50]

Finally, a sixth approach to consider is harnessing established private sector mechanisms to encourage compliance with the obligations. This would involve embedding and operationalizing the principles in the due diligence procedures employed by especially prominent investors (such as sovereign wealth funds and large holding companies) and banks, risk-assessing entities (such as credit rating companies), and insurance companies underwriting cyber risks. Some of these actors are already engaging in such practices, albeit in a less structured and comprehensive manner. They could be encouraged to develop checklists and audit mechanisms to assess compliance with proposed obligations and reflect this in their business decisions.

TABLE 5
Options for Anchoring Obligations and Incentivizing Adherence

Platforms for Anchoring Obligations
• Unilateral or collective declarations by governments and/or corporations pledging to honor and promote these obligations • Formal bilateral and multinational trade arrangements and/or less binding international documents (by G7 and G20 communiques and/or the GGE, OEWG, WTO, ITU, OECD) • Technical standards–setting organizations both domestic (for example, NIST) and international (for example, ISO, IEC) • Corporate-led processes (for example, Tech Accord, CoT) or multi-stakeholder processes (for example, through the OECD Global Forum) • Dedicated CSR/ESG initiative to promote high security and supply chain integrity standards, potentially in collaboration with the Institute for Supply Management
Additional Incentives for Adherence
• Deny outliers access to government contracts or national markets • Introduce mutual accreditation and certification mechanisms for approved vendors, products, and services • Create reputational benefits for those in compliance (and stigmatize those who are not) • Harness private sector mechanisms, including the due diligence procedures of key stakeholders, to encourage compliance

Arrangements for Verification and Discouraging Noncompliance

There is universal appeal to developing clear and transparent principles and norms for protecting the integrity of ICT/OT supply chains. However, reaching consensus on, securing broad buy-in, and ensuring implementation of them is bound to prove very challenging. While there could initially be some compromise on the scope of participation, the appeal and utility of the obligations ultimately depend on having credible mechanisms to verify compliant and noncompliant behavior and to reward the former and/or penalize the latter. Such mechanisms are essential to enhance trust, encourage buy-in, and deter cheating. Without verification, norms may not only be meaningless but also counterproductive.

Many observers believe it is practically impossible, technically speaking, to attain full confidence in the integrity of ICT/OT products and services. They submit that sophisticated players will always be able to subtly intervene in the ICT/OT supply chain in a manner that will make it exceptionally difficult to detect and, even more challenging, to reliably attribute the intervention. They note a huge barrier in the ability to distinguish between innocent errors/flaws and deliberate interventions (partially aided by insiders).[51] Therefore, the argument goes, effectively verifying restraints on tampering with products and services is beyond reach today and unlikely to be more feasible any time soon.

What these assessments do not disprove, however, is that states and corporations could adopt at least some obligations to help build confidence in the integrity of the supply chain. The mere public commitment by governments as well as corporations to abide by the proposed principles would by itself be verifiable, setting apart those that do subscribe to these norms from those that do not. Additionally, once states and corporations make public some of their obligations in this realm (for example, those aimed at increasing transparency and accountability), they inevitably open themselves up for public (and for that manner also peer) scrutiny thereby at the very least providing outside monitors a clear benchmark against which to assess their actual behavior.

Moreover, the broader verification question is not whether one could reach a high certainty that every sophisticated intervention would be detected and determined to be intentional. Rather, the question is whether actual or would-be perpetrators could safely assume that interventions would not be detected, identified as intentional, and correctly attributed. Transparency and accountability measures certainly reinforce this deterrent effect even though they are not a panacea.

Leverage Quality Assurance Best Practices

On the technical side, discovering the origins of interventions could become easier due to the increasingly common best practice of building a chain of custody and embedding “traceability” functions into both hardware and software supply chains.[52] This practice began for quality assurance purposes, but could now serve as a deterrent against noncompliance with the proposed obligations. Traceability requires the comprehensive, systematic documentation of all critical inputs into the development, production, updating, upgrading, and modification of products. It could rely, in part, on distributed ledger (aka blockchain) technology to enable real-time tracking, information sharing with other parties in the supply chain and customers, and the tracing of discovered anomalies back to the point of origin. Traceability enables vendors and potentially subsequent investigators to track down the origins of all components and the standards that subcontractors apply to them. The rigorous certification of suppliers and subcontractors and corresponding audit procedures greatly enhance traceability. Together, the practices make it easier to engage in root cause analysis and to determine the origin of an intervention, who carried it out and why.

Traceability thus stands out as an important means of increasing the feasibility of normative restraints against intentional interventions. This is regardless of whether a comprehensive, foolproof verification regime remains elusive. Once in place, transparent, traceability measures will go a long way toward reassuring others about corporations’ sincerity in committing to higher industry standards for ICT/OT products and services.

Solicit Governmental Input

Several intelligence, law enforcement, homeland, and cyber security agencies around the world certainly possess the pertinent expertise as well as information (both circumstantial and case specific) to help determine whether discovered vulnerabilities originate in deliberate supply chain interventions, or in unintentional flaws. They could for example tap their resources to determine whether a discovered anomaly was an isolated case or affected all "copies" of a product or service.[53] Their prowess in technical forensics could similarly inform such analysis, helping confirm or refute suspicions of interventions or deliberate creation of vulnerabilities. And they might also bring to bear their unique access to intelligence to provide circumstantial and even case specific evidence that could complement a technical investigation.

The biggest challenge in mobilizing governmental resources to help address the verification challenge does not lie with governments' capacities but rather with their will to undertake such a mission. Two barriers that may dissuade them from performing this role are particularly noteworthy. First, some governments may be politically reluctant to make charges against others, thereby opening themselves to reprisals. Second, governments naturally worry about compromising sources and methods of intelligence. Yet intelligence agencies have always found creative ways and modalities for sharing (or leaking) intelligence in the interest of promoting other policy goals to counter proliferation, terrorism, and drug trafficking and are widely believed to have done so more recently in several cyber related cases. Some governments have also directly cooperated in investigating and combating harmful cyber actions. It is certainly conceivable that they can similarly cooperate in the interest of enhancing supply chain integrity (for example by discreetly informing the deliberations of the independent assessment body proposed below). Even more importantly, since government officials, especially in the United States, have often alleged foreign foul play in the supply chain, it would be reasonable to expect and important to demand that they back up such allegations to help inform deliberations of objective experts assessing the merit behind such concerns.

Establish an Independent Assessment Body

Such expert deliberations could take place under the auspices of a new private or public-private body that would be set up to identify, diagnose, and engage in root cause analysis of significant supply chain flaws and vulnerabilities. In its most ambitious form, the institution could test and rate the security of ICT/OT products. This could be a commercial service (similar to UL or others used, for example, to test engine emissions) or run as a voluntary global or regional public service. The body could also certify that products meet soft regulatory or other cybersecurity requirements in order to qualify for certain types of public and/or private contracts. It could draw inspiration from the European experience in trying to move from nationally based bodies to a broader European-based IT certification authority. Tapping the broad global community of experts who would (and could be encouraged to) weigh in on any publicly revealed incident could provide another useful source of insight (a permutation on the crowdsourcing concept).

Another perhaps more practical option would be an independent *technical* body designed to assess claims of manipulation or reckless disregard for cybersecurity in commercial off-the-shelf ICT/OT products and services. Its mission would be to help substantiate or dispel the claims or concerns. It could determine whether detected anomalies should be attributed to more than innocent mistakes, using a standard of plausibility rather than a definitive assessment. However, the body would not be a politically inspired organization or a standard verification institute, but rather an ad hoc service to analyze cases voluntarily referred to it. Producers, no doubt, could be tempted to exploit such a mechanism to cast doubts on competitors' products and services. But they might also fear retaliation for such behavior. Thus, serious vendors are likely to seize on the opportunity provided by this mechanism to reassure others (customers and governments alike) of their intentions and the credibility of their security practices upon discoveries of weaknesses and vulnerabilities in their products, even in the absence of allegations that they have not lived up to their obligations. By sharing technical and procedural information with the body, these vendors could both help their case and strengthen the incentive for others to do the same when concerns pertaining to them arise.

The body could, in turn, share its findings with those who were inspected and those who raised the concerns or made the allegations. Perhaps in a sanitized form such findings also could be shared with the general public to reassure them about the sincerity of the exercise, thereby enhancing their trust in the ICT/OT product and in industry best practices as a whole. The body could and certainly should also share broadly the generic lessons learned from various assessments with corporations, thereby helping them to make risk-based decisions and prioritize efforts to enhance the integrity of their products. The fact that corporations would be willing to engage with such a body would be a public confidence-building measure in its own right.

Borrowing insights from the arms control domain, the founding partners to the technical body should decide on its authority to review claims, subjecting such claims either to presumption of approval ("red light") or denial ("green light"). Both practices having been historically used in treaties such as the Chemical Weapons Convention ("red light") and the Comprehensive Test Ban Treaty ("green light"). In the latter case, it will be up to those who allege that a security concern may be a case of deliberate action or gross negligence to persuade a certain percentage, to be determined, of other members about the need to undertake the technical review before it could proceed. In a "red light" system, the presumption would be for each complaint to be automatically referred to review by the technical body, which could be stopped only if a compelling case namely a majority (the percentage of which once again has to be set in advance) could be marshaled against it on the grounds that this would be inappropriate or unwarranted in that particular instance.

Applying this relevant experience to the supply chain verification challenge would require that corporations commit in advance to refer cases to this expert body and open themselves to in-depth scrutiny whenever warranted. Such willingness would inevitably depend on striking a fine balance on the level of transparency (internally, and separately externally) required for its successful performance. Both to conduct credible deliberations assessments and to endow its subsequent findings with public credibility, while also protecting legitimate intellectual property and liability corporate concerns.[54]

Naturally, the founding members of such a body would need to develop and agree upon additional rules guiding how this entity would operate. Presumably, founders would in the main come from the ranks of vendors. Ideally, founders would invite some academic or independent institutions as well as independent experts to join, as this could greatly enhance the body's credibility. Governmental experts could conceivably be invited to partake in some of its deliberations as observers. Funding for operations of this body should come from modest contributions from participating vendors who ought to contract with a law firm, association, or nonprofit organization to serve as a convener. Regardless of the specific institutional arrangements selected, for each specific assignment the technical assessment should draw on a handful of experts from a pre-accredited pool. The pool could be drawn mainly, but preferably not exclusively, from the ranks of members of the body, thereby reducing costs, increasing the chance of availability, and ensuring the objectivity of the analysis. These experts would operate according to pre-agreed generic guidelines on mission, mandate, scope, analytical criteria, remuneration, and reporting of their findings to the members. In addition, they would be bound by strict ethics and confidentiality provisions that would, inter alia, stipulate that no public report on their findings would be issued without the explicit consent of the inspected corporation.

Some governments and corporations might seek an even more stringent verification regime for the obligations proposed—for example, by setting up a legally or politically binding institutional verification arrangement. While the desire to build a stronger incentive structure for compliance is understandable, this idea and similar ones would be impractical and probably even counterproductive. There would be formidable technical and procedural difficulties in making such an arrangement credible, partially because any exercise that pins blame on corporations would inevitably sour the prospects of objective and widespread collaboration and could rapidly escalate into a politically toxic controversy. The more modest approach proposed here wouldn't stop states from engaging in political maneuvers over the supply chain. However, doing so would jeopardize the benefits of multilateral and multi-stakeholder cooperation to enhance ICT/OT supply chain integrity.

TABLE 6

Possible Mechanisms for Verifying Compliance

Possible Mechanisms for Verifying Compliance
• Leverage best practices for enhancing the performance, safety, and quality assurance of products and services (for example, certification of suppliers and subcontractors, audits, chain of custody, traceability, root-cause analysis) to aid the investigation of discovered vulnerabilities • Invite governments to support and expeditiously inform private sector analysis of vulnerabilities and, as practical, also their origins • Establish an independent, international mechanism to technically analyze and diagnose discovered vulnerabilities

The Way Ahead

Experience to date suggests that it will be difficult to gain wide international acceptance of ambitious norms. There are too many states and corporations with intensely too many conflicting interests to reconcile—both domestically and internationally. Even a strong incentive structure for compliance will not prevent all those committed to the obligations from violating certain norms at certain times. This is because there are many actors with diverse incentives to intervene and limited mechanisms exist for verifying and rewarding good behavior.

Furthermore, even if leading states and corporations accept and adhere to the norms, attaining total trust in the integrity of the ICT/OT supply chain will still be impossible. Suspicions and anxiety—fueled by well-founded but sometimes inflated concerns and commercial and political interests—will always persist.

This does not mean, however, that significant efforts toward protecting the integrity of the supply chain will not have positive results. Efforts already under way indicate that many people believe we are better off with some norms than none at all, even if it is difficult to verify compliance. Carnegie's interviews with a wide range of stakeholders confirmed this view. What was also clear from the interviews is that complementary norms for both governments and corporations are necessary to strike a proper balance between national security and law enforcement interests and those of the digital economy.

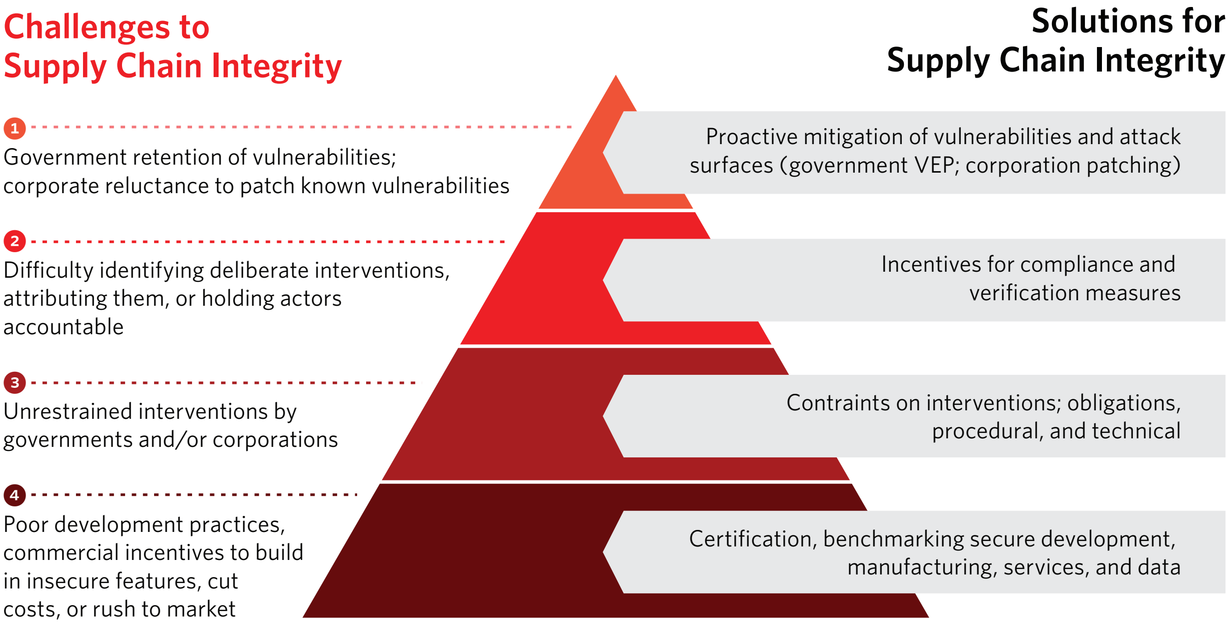
Broadly speaking, governments must be extremely selective and cautious in carrying out supply chain interventions. Governments should refrain from making systemic interventions and only use discrete interventions after thoroughly analyzing and weighing the risks involved. If and when they do engage in such interventions, governments must employ considerable safeguards to ensure that their actions are highly localized, confined to agreed-upon parameters, and tempered by time and physical constraints. Governments otherwise inclined would need to understand and internalize that even if they could keep interventions secret, they still create profound risks to the integrity of the supply chain and, ultimately, undermine trust in the digital economy.

Likewise, corporations offering ICT/OT products and services must do everything in their power to enhance the integrity of their supply chains—not only to serve their diverse commercial interests but also those of the digital economy writ large. They should take elaborate measures to design, develop, produce, and acquire highly secure products and support them with equal vigor throughout their life cycle. In addition, they must commit to increasing the transparency of their security practices and enable a level of scrutiny by outside experts. They must do this to reduce technical, commercial, or political concerns or allegations that could seriously undermine trust in their products, the industry, and the entire digital ecosystem. Naturally, this calls for both collective and individual corporate efforts.

Figure 2 summarizes the core challenges to ICT/OT supply chain security and the proposed holistic solutions to overcoming them.

FIGURE 2

A Holistic Approach to Ensuring Supply Chain Integrity


Challenges to Supply Chain Integrity
Solutions for Supply Chain Integrity
1
Government retention of vulnerabilities; corporate reluctance to patch known vulnerabilities
2
Difficulty identifying deliberate interventions, attributing them, or holding actors accountable
3
Unrestrained interventions by governments and/or corporations
4
Poor development practices, commercial incentives to build in insecure features, cut costs, or rush to market
Proactive mitigation of vulnerabilities and attack surfaces (government VEP; corporation patching)
Incentives for compliance and verification measures
Contraints on interventions; obligations, procedural, and technical
Certification, benchmarking secure development, manufacturing, services, and data

Of course, technical measures to enhance supply chain integrity must be complemented by supporting policies. But given that reaching a global consensus on these policies will be a long-term effort, it is crucial to quickly gain the buy-in of several governments and corporations, especially major suppliers of ICT/OT products and services in the United States, leading European nations, and China.

Some might be inclined to think that persuading the Chinese government and Chinese corporations to participate would be the most difficult challenge to overcome. Yet, it is not clear that this is the case, for several reasons. First, it is worth recalling that Chinese governmental experts did sign on to the explicit language on supply chain integrity contained in the 2015 GGE report.[55] Second, Chinese governmental and corporate interests in becoming global vendors of ICT products and services might require them to be more forthcoming in building trust than they have been to date. The broad campaign, by U.S. President Donald Trump's administration and the U.S. Congress, against Chinese telecommunications and related products and services may have awakened Chinese government and corporate leaders to the urgent need to find a constructive (and non-embarrassing) way of reassuring the global community of the integrity of their products. One small indication of this is the recent decision by Huawei join the Paris Call for Trust and Security in Cyberspace,[56] as well as the interest taken by Chinese vendors in the work of the OECD Global Forum on Digital Security for Prosperity.[57] Additionally, the option offered here of distinguishing between domestically oriented interventions in the supply chain and international ones could offer a way for China to meet the regime's internal information requirements while still reassuring the world that the Chinese government and vendors conform to a different standard internationally. Finally, it would unquestionably be easier to get Chinese actors on board if they would be assured some reciprocity or rewards for adopting such commitments. Of course, the issue of reciprocity could raise interesting challenges in Washington, where multiple interests may animate the dispute over ICT supply trustworthiness, and where government agencies have long wished to retain latitude for engaging in supply chain interventions. It is very instructive in this respect that neither the Chinese nor the U.S. governments (both presumably committed to the principles pertaining to the supply chain integrity agreed in the 2015 GGE) have thus far joined scores of nations, including every member state of the European Union and numerous others, in the Paris Call.

Transforming the proposed, aspirational obligations into a widely accepted, operational framework would thus require a sustained effort to persuade the key stakeholders or at least a quorum thereof to engage in such an undertaking. This would require taking some preparatory steps before proceeding. A relatively noncontentious first step is to have all interested parties issue a uniform declaratory statement, such as joining the Paris Call and proclaiming that "actions that systemically or broadly destabilize or undermine confidence in the ICT/OT supply chain are unacceptable. The signatories commit to refraining from undertaking these actions and to take concrete positive actions, individually and collectively, to further enhance trust in these products and services, as well as to impose consequences on all those who fail to adhere to and comply with this pledge." This declaration should ideally become universal—open to endorsement by all states and corporations. It could also be incorporated in bilateral or multilateral trade agreements.

All parties who formally subscribe to such a pledge (by a certain date) could then come together to affirm and operationalize an agenda. They would call on other states and corporations to also make the pledge and begin to work together. States and corporations could separately and/or together build a code of conduct (or charter of trust) in the ICT/OT domain. The concrete suggestions made in this paper for both substantive commitments as well as implementation options could then become, by agreement, the agenda for discussions.

The next steps could include international dialogue; further vetting, refinement, and prioritization of obligations; possible expansion of the scope to include data and algorithms; and the building of synergies with other efforts to protect the integrity of the ICT supply chain. Such broad open-ended dialogue could perhaps take place also under UN auspices, within the GGE as well as the OEWG.[58] *International dialogue* is necessary to confirm that the logic underlying the proposed obligations is compelling enough to motivate states and corporations to comply with them. In an international environment where nationalism and geopolitical and economic rivalries are on the rise and preexisting multinational and multilateral arrangements show great strains, the prospects for new cooperative arrangements appear increasingly dim. Moreover, implementing the obligations will not be cost-free for either governments or corporations. And governments might have to forego certain supply chain operations related to intelligence and/or military activities. Each government and corporation involved will thus have to carefully weigh the pros and cons of, and conditions for, committing to the obligations. This paper attempts to help inform this debate in three ways: by portraying the consequences of a world without meaningful norms in this domain; by proposing obligations that account for national security imperatives; and by proposing an incentive structure and verification regime that would benefit those that comply and exclude holdouts and cheaters.

In this context, it is important to underscore an inherent opportunity in the marketplace. Less than a handful of governments possess the sophistication and access to undertake systemic supply chain interventions in the ICT/OT domain. Similarly, the number of companies able to provide equipment for the backbone of the internet and 5G networks is relatively small. This means that both groups wield disproportionate influence on their own extensive supply chains and on the overall feasibility of the obligations proposed. Hence, if a mere handful of those can be won over, others, including subcontractors, would be heavily inclined to come on board rather than face severe repercussions.

Dialogue should also focus on the form commitments should take. Do states and corporations require different formats or mechanisms? Would states and corporations be expected to make unilateral statements of commitment, or would commitments have to be based on some form of reciprocity between states, between corporations, and between states and corporations? If so, in what sequence? Finally, must these commitments be explicit, in a way that acknowledges they are engaged in certain practices? Could they realistically be made without reference to what others commit to do? Of course, adoption of the proposed obligations cannot be expected before they are subjected to *further vetting* and *refinement* for both technical merit and bureaucratic (and occasionally political) and commercial viability in different cultures and political systems. Carnegie is already undertaking this line of work and intends to sustain it in the coming months. We encourage others to act in this space, too. We would be pleased to collect proposals and analyses and share them with interested parties, and/or publicly post them.

It will also be necessary to *prioritize* among the obligations. Some obligations seem more important, or at least more time-sensitive, than others—for example, the commitment to refrain from systemic or broad backdoor interventions into the ICT/OT supply chain and the commitments to increasing transparency and accountability. These commitments are urgently needed to arrest the increasing balkanization of the marketplace and to rebuild trust in products and services. They should be considered foundational obligations that states and corporations must subscribe to. Otherwise, some states and corporations might be inclined to cherry pick other less important, easier obligations to adopt.

Before proceeding, it might also be worthwhile to *expand the scope* of the obligations to capture data and algorithms, which are assuming greater importance for ICT/OT products and services and could be similarly subjected to consequential manipulation. The lines between hardware, software, data, and algorithms are being increasingly blurred.[59] For example, designs to be printed in 3D printers, not just the printers themselves, are attackable, and the components end up in a supply chain. Similarly, training data employed in machine learning, graphs, and neural networks make it necessary to consider data as a part of the supply chain as well. Data and algorithms are not traditionally considered part of the ICT/OT supply chain, but the concerns, dilemmas, and recommendations surrounding hardware and software seem applicable in these areas as well. Naturally, expanding the scope raises new complications and challenges that greatly exceed the scope of this paper. For example, greatly expanding both the number of players that would have to be involved in such deliberations as well as the issues they would have to tackle. But these technological and market trends are already having consequences, not in the least in beginning to undermine trust in the introduction and broad dissemination of new products and applications. The crisis of confidence will loom larger in the near future if correction action is not taken now.

At the same time, notwithstanding some unique aspects of supply chain integrity on the ICT/OT domain, there are many aspects of the supply chain challenge in this domain that are common to other globally significant industries. Some industries (and governments) have been dealing with such challenges for much longer than the cyber industry. See Appendix 1 for one instructive case in point (fake pharmaceuticals). There is thus much room for cross-industry discussion of the remedies to such challenges, and perhaps some joint action as well. This reinforces the potential value of collaborating with the Institute of Supply Management and similar institutions around the world in identifying best practices, raising awareness, educating and training, and conducting outreach to other stakeholders. Similar logic drives the earlier recommendation to reach out early to financial institutions, holding companies, and insurance and credit rating companies, to launch the dialogue with them on how they could support a process (in which they have a vested interest) designed to minimize cyber risks.

Finally, the high-level obligations proposed should be considered with other initiatives in mind. The obligations by themselves will not suffice to overcome the existing trust deficit in the supply chain for ICT/OT products and services, even if they achieved broad endorsement and compliance. Ultimately, they would have to be both combined and *aligned with vital other efforts* already under way to strengthen confidence in the integrity of the ICT supply chain.[60] These efforts obviously must go hand in hand with efforts to build resilient architecture that is less sensitive to those interventions that cannot be ruled out, such as the approach conceived by the UK National Cyber Security Center for 5G networks.[61] Together with these other laudable efforts (which thus far do not address systematic discussion of norms), the recommended obligations could become the building blocks of a global supply chain integrity regime.

Table 7 below summarizes some options for moving ahead on this front.

TABLE 7
Possible Next Steps

Optional Steps for Further Development
• Outreach and briefings to individual governments and corporations to seek buy-in for core principles and encourage pledges to honor them—both unilaterally and collectively in governmental settings like the G7/G20, UN GGE and OEWG, corporate-led processes (for example, Tech Accord, Charter of Trust), and multi-stakeholder processes (for example, OECD Global Forum) • Engage with private sector stakeholders (financial sector, insurance, and so on) on developing further incentives, including promoting cyber risk assessment and management considerations in due diligence processes • Initiate a process to develop mechanisms and techniques for verification and operationalization of standards, including through engagement with standards-setting domestic (such as NIST) and international organizations (like ISO, IEC) • Explore options for launching a CSR/ESG initiative to further operationalize these commitments and build mechanisms for their effective implementation. In this context aim to anchor the corporate responsibility in the Institute for Supply Management (ISM) Principles of Sustainability and Social Responsibility

Finally, it seems advisable to conclude with a longer-term perspective. Building a healthy digital economy depends not merely on enhancing individual supply chains but on the creation of a secure supply chain network, in fact, an entirely globalized and trustworthy digital economy ecosystem. A truly ambitious goal for sure, one that will take both strenuous efforts and an extended period to approximate. Yet one that ought nevertheless to guide and inspire us as we take whatever baby steps prove practical today and tomorrow.

Appendix 1: Supply Chain Security: The Analogy to Counterfeit Pharmaceuticals

Wyatt Hoffman

Counterfeit pharmaceuticals have become one of the most profitable criminal enterprises, raking in around $200 billion annually by some estimates.[62] For decades, the pharmaceutical sector has had to deal with this threat that is

- *escalating in complexity*, with the acute challenges of securing globalized supply chains;
- *grave in consequence*, both in terms of financial costs and global public health impacts; and
- *persistent*, with progress met by the constant evolution of malicious threats.

Of course, the challenge of securing pharmaceutical supply chains against predominantly profit-motivated criminal threats differs in important ways from that of securing ICTs against more diverse threats and unique modes of intervention and propagation. Nevertheless, the pharmaceutical sector's long experience with the core task of ensuring the integrity of products is instructive for the ICT sector facing a challenge of similar scope, scale, and consequence.

The Common Challenge of Supply Chain Risk Management

The same forces of globalization and disruptive technologies that have shaped ICT supply chains have transformed those of numerous industries now facing dynamic, transnational threats. Nowhere have the stakes been higher than the pharmaceutical sector. Pharmaceutical supply chains have rapidly grown in complexity, with numerous stages and many actors involved, often with materials sourced from or moving through multiple countries. States with inadequate regulation or weak enforcement create opportunities for criminals to intervene and insert corrupted products. These can occur surreptitiously at different stages: sourcing of ingredients and materials, fabrication, shipment, and distribution. Counterfeit or otherwise substandard products account for around 10 percent of drugs in developing states on average, and through compromised supply chains, they reach more secure markets in developed states.[63]

ICTs are often characterized as an ecosystem. This apt description points to an additional facet of this analogy in the potential cascading or corrosive effects that compromised supply chains can have on the entire health of the ecosystem. Of course, in both cases, consumers bear the immediate impacts of compromised supply chains. Estimates of the number of deaths per year linked to substandard or falsified drugs—either ineffective against disease or directly harmful—are in the hundreds of thousands.[64] Beyond this immediate harm, the widespread introduction of compromised products has cumulative deleterious impacts on health, as substandard drugs fuel antibiotic resistance and create breeding grounds for diseases that spread to other, more secure populations.[65] In a similar manner, compromised ICTs can introduce vulnerabilities and create new attack vectors to reach otherwise secure systems.

Less visible are the corrosive effects of lost confidence in suppliers, products, and services. Like the ICT ecosystem, healthcare services depend on *trust*. Consumers cannot readily assess the quality or composition of a drug and thus depend almost entirely on trust in suppliers. Beyond the reputational damage to individual corporations, substandard drugs erode broader public confidence in healthcare.[66] It is becoming ever more apparent that the compromise of ICT products can produce similarly lasting consequences in the form of lost confidence in functions and services crucial to society.

Solutions From the Pharmaceutical Sector

Pharmaceutical manufacturers will be intimately familiar with the challenges facing ICT vendors: managing vast networks of suppliers and subcontractors; tracking materials and products and communicating this information in real-time; ensuring security along every stage in the process; and detecting and tracing discovered flaws to the point of origin. Some solutions implemented by pharmaceutical manufacturers can map directly onto the ICT supply chain, while others offer models and principles for initiatives, regulation, and collaboration.

Technological—A range of technologies allow pharmaceutical manufacturers to track and trace materials and products in real-time throughout the supply chain (for example, RFID tags and other unique identifiers), record this information and transmit to relevant parties, and detect and prevent attempts to tamper with products in the supply chain or en route to customers. ICT vendors have already begun to explore and implement similar measures for continuous visibility and could learn from pioneering efforts in the pharmaceutical sector—including, notably, the application of blockchain technology (among others) for supply chain management.[67]

Industry initiatives—Pharmaceutical corporations have long recognized the shared nature of the threat from counterfeits. Established in 2002, the nonprofit Pharmaceutical Security Institute now includes thirty-three manufacturers around the world and provides a platform for sharing information on counterfeit threats and public resources to identify safe medicines.[68] Numerous individual manufacturers have created dedicated laboratories to detect and mitigate counterfeit threats, often providing support for international law enforcement action.[69]

Policy and regulation—Regulations in numerous states creating requirements for "mass serialization" and track-and-trace measures have played an important role in prompting technological solutions by industry.[70] This includes the European Union's Falsified Medicines Directive in 2011 and the U.S. Drug Supply Chain Security Act, passed in 2013. The latter requires corporations to "build an electronic interoperable system to identify and trace certain prescription drugs."[71]

International cooperation—The World Health Organization launched its Global Surveillance and Monitoring System in 2013, providing a common mechanism for participating regulatory authorities and clinical personnel to report detected counterfeit products.[72] Numerous other initiatives help build regulatory capacity in developing states.[73] International law enforcement cooperation has proven invaluable in disrupting counterfeit threats, including the annual Operation Pangea led by INTERPOL, which involved 123 countries in 2017.[74]

Takeaways From the Pharmaceutical Experience

While this is merely a cursory survey, it is worth concluding with a few tentative observations:

1. **Complementary efforts by corporations and governments are needed**. There is no silver bullet for supply chain security. Better corporate practices and the implementation of technical solutions have been essential, but these can only go so far in the absence of government action against persistent threats. Private sector initiatives such as the International Federation of Pharmaceutical Manufacturers and Associations have supported governments with developing effective regulation and enforcement.[75] And governments can assist the private sector in developing common solutions, like the U.S. Food and Drug Administration's pilot project exploring blockchain applications and other technical measures for supply chain risk management.[76]
2. **Supply chain risk management is good for business**. Corporations tend to view investments in risk management as a drain on precious resources. Such investments result in significant savings from better detection and prevention of counterfeits that cut into profits and force costly remedies such as mass recalls. Yet evidence suggests better supply chain management has significant ancillary benefits that contribute to competitiveness by improving overall efficiency, quality, and responsiveness to customers.[77] Moreover, these savings multiply with the adoption of common standards that streamline transactions, quality assurance, and compliance with regulations and requirements.[78]
3. **Harmonized standards are essential to security and trust in the ecosystem**. A study by the nonprofit GS1 argued that proprietary solutions developed in isolation lack the interoperability essential to promoting cooperation and trust throughout the healthcare value chain.[79] GS1's set of standards for supply chain visibility and traceability has guided industry efforts and capacity-building initiatives (such as the U.S. Agency for International Development's Global Health Supply Chain Program), and enabled progress toward harmonized regulatory requirements across numerous countries.[80] A common set of industry practices and technologies both underpins multi-stakeholder collaboration against threats (for example, allowing for rapid detection and response to criminal activity) and creates a source of broader confidence in the integrity of healthcare products.

4. **Protecting the supply chain is an ongoing struggle**. Supply chain security is not an end state for corporations to reach. Rather, as the pharmaceutical sector can attest to, constant vigilance is needed to manage evolving risks. Criminal enterprises innovate their tactics to overcome innovations in security. And they take advantage of market opportunities such as large-scale initiatives to combat emerging diseases.[81] Only through collaboration and the pooling of insights can industry and its partners keep abreast of threats.

About the Author

Ariel (Eli) Levite is a nonresident senior fellow in the Nuclear Policy Program at the Carnegie Endowment for International Peace. Prior to joining the Carnegie in 2008, Levite was the principal deputy director general for policy at the Israeli Atomic Energy Commission from 2002 to 2007. He also served as the deputy national security adviser for defense policy and was head of the Bureau of International Security and Arms Control (an assistant secretary position) in the Israeli Ministry of Defense.

Acknowledgments

The author wishes to acknowledge the invaluable contributions of his current and former colleagues at Carnegie's Cyber Policy Initiative, including Jon Bateman, Kate Charlet, Wyatt Hoffman, Tim Maurer, George Perkovich, and Kamaal Thomas. Additionally, gratitude goes to Jon Boyens, Mark Chandler, Richard (Dickie) George, Cristin Goodwin, Anthony Grieco, Robert Hannigan, Steve Lipner, Bobbie Stempfley, Yaoz Talshir, and Eric Wenger for their outstanding insights and suggestions, as well as comments on drafts of this paper. Many others who have graciously given advice and comments wish to remain anonymous for now. The paper's content is the sole responsibility of the author and does not necessarily represent the views of any other individual or institution.

Carnegie's Technology and International Affairs Program is thankful for support from the following foundations, governments, corporations, and individuals, which help make our work on cyber policy possible: the Hewlett Foundation, the Carnegie Corporation of New York, Cisco Systems Inc, Microsoft, Bank of America, the Commonwealth Bank of Australia, Ken Olivier and Angela Nomellini, and trustees of the Carnegie Endowment for International Peace. Carnegie is honored to work with donors and partners that share its institutional goals and mission. Donors do not review drafts, influence the selection of project participants, or influence the findings and recommendations of work they may support.

Notes

1 There is no universal definition of ICT. In this paper, ICT includes industrial control systems (ICS) products and routers/switches, other control systems, servers, database and operating software, laptops, personal computers, and mobile devices. Consumer Internet-of-Things products are explicitly excluded from consideration here because they are numerous and typically have too little security built into them in the first place, and inferior integrity of products and services in this category is bound to produce far smaller strategic and economic impact.

2 Andy Greenberg, "Meltdown Redux: Intel Flaw Lets Hackers Siphon Secrets From Millions of PCs," *Wired*, May 14, 2019, https://www.wired.com/story/intel-mds-attack-speculative-execution-buffer/.

3 This study uses a hybrid definition of the "supply chain." It captures the network of resources (hardware, software, data, and algorithms) integrated into ICT/OT products and services throughout their entire life cycle. While individuals, organizations, and activities customarily captured in supply chain definitions are excluded here, the inclusion of data and algorithms represents an expansion of traditional supply chain definitions.

4 Ongoing powerful cases are being made for both why the prosperity of the digital economy hinges on the availability of strong encryption standards but also for the opposing viewpoint why vital national security requirements can only be met by building back doors into these standards. This debate is not included in the scope of this paper.

5 Among the valuable research in this area, one paper, in particular, that provides an easy-to-understand comprehensive survey of the issues involved is Scott Charney and Eric Warner, "Cyber Supply Chain Risk Management: Towards a Global vision of Transparency and Trust," Microsoft White Paper, July 26, 2011, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REXXtT.

6 Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg Businessweek*, October 4, 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

7 Tara Beeny, Jennifer Bisceglie, Brent Wildasin, and Dean Cheng, "Supply Chain Vulnerabilities From China in U.S. Federal Information and Communications Technology," Interos Solutions, April 2018, https://www.uscc.gov/sites/default/files/Research/Interos_Supply%20Chain%20Vulnerabilities%20from%20China%20in%20U.S.%20Federal%20ICT_final.pdf.

8 James R. Clapper, "Statement for the Record: Worldwide Cyber Threats," House Permanent Select Committee on Intelligence, September 10, 2015, https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf.

9 Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *New York Times*, September 5, 2013, https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html. See also, Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York, NY: Houghton Mifflin Harcourt, 2014).

10 See "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," New America, June 29, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/; Maytak Chin, Cong Liu, and Xiaoyan Zhang, "China's Cybersecurity Law," Reed Smith LLP, January 11, 2018, https://www.reedsmith.com/en/perspectives/2018/01/chinas-cybersecurity-law; Scott Shackelford, Eric Richards, Anjanette Raymond, Jaclyn Kerr, and Andreas Kuehn, "Decrypting the Global Encryption Debate," *Huffington Post*, October 20, 2016, https://www.huffingtonpost.com/entry/5808d3f9e4b00483d3b5d0bf; and Derek Hawkins, "The Cybersecurity 202: U.S. Tech Firms Slam Australian Bill That Could Weaken Encryption and ICT Products More Broadly," *Washington Post*, October 19, 2018, https://www.washingtonpost.com/

news/powerpost/paloma/the-cybersecurity-202/2018/10/19/the-cybersecurity-202-u-s-tech-firms-slam-australian-bill-that-could-weaken-encryption/5bc8f0a71b326b7c8a8d1a7e/?utm_term=.9971d6a97654.

[11] See, for example, the 2011 publication of the "Supply Chain Risk Management Council: Supply Chain Risk Management: A Compilation of Best Practices," available at: http://www.scrlc.com/articles/Supply_Chain_Risk_Management_A_Compilation_of_Best_Practices_final[1].pdf. In the ICT/OT space, see for example the seminal publication by NIST, which is also facilitating much work on supply chain integrity, as well as the BSA's 2019 publications "Framework for Secure Software," https://www.bsa.org/reports/bsa-framework-for-secure-software and "BSA Principles for Good Governance: Supply Chain Risk Management," https://www.bsa.org/files/policy-filings/07172019bsasupplychainprinciples.pdf.

[12] "ENISA Work in the Area of Certification," European Union Agency for Cybersecurity, https://www.enisa.europa.eu/topics/standards/copy_of_certification.

[13] "Common Criteria Certification," National Cybersecurity Agency of France, https://www.ssi.gouv.fr/en/certification/common-criteria-certification/.

[14] U.S. Department of Homeland Security, "DHS and Private Sector Partners Establish Information and Communications Technology Supply Chain Risk Management Task Force," October 30, 2018, https://www.dhs.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology.

[15] This analysis should not be interpreted to mean there are no considerations that weigh against supply chain interventions. Some of them are actually mentioned in the paper. But the various rationales to undertake such attacks listed above are serious enough to make abstinence or even extreme restraint in carrying out such operations into a nontrivial proposition. All the more so if it assumes the form of a commitment anchored in an international obligation.

[16] "Dragonfly: Western Energy Companies Under Sabotage Threat," Symantec, June 30, 2014, https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear.

[17] "Lenovo Settles FTC Charges It Harmed Consumers With Preinstalled Software on Its Laptops That Compromised Online Security," Federal Trade Commission, September 5, 2017, https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled.

[18] Andy Greenberg, "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/.

[19] Andy Greenberg, "Meltdown Redux."

[20] "Operation Cloud Hopper," PwC, April 2017, https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.

[21] For several other recent notable examples of widespread vulnerabilities or security compromises discovered see: Richard Waters, "Intel Reveals Flaw in Chips That Makes Them Vulnerable to Hackers," *Financial Times*, May 14, 2019, https://www.ft.com/content/d60cda42-7699-11e9-be7d-6d846537acab; Dan Goodin, "Apple Pushes Fix for 'FacePalm,' Possibly Its Creepiest Vulnerability Ever," Ars Technica, February 7, 2019, https://arstechnica.com/information-technology/2019/02/apple-pushes-fix-for-facepalm-possibly-its-creepiest-vulnerability-ever/; and Lily Hay Newman, "A Cisco Router Bug Has Massive Global Implications," *Wired*, May 13, 2019. https://www.wired.com/story/cisco-router-bug-secure-boot-trust-anchor/; Andy Greenberg, "A Mysterious Hacker Group Is on a Supply Chain Hijacking Spree," *Wired*, May 3, 2019, https://www.wired.com/story/barium-supply-chain-hackers/.

[22] We submit that intervention that occurs in multiple exemplars of the same item destined for one customer could still be considered ad hoc provided it does not materially affect other customers of the same product.

[23] Such a norm therefore would explicitly pertain to both pre- and postdelivery of products and services.

[24] Since the first drafts of this paper containing this recommendation were informally circulated in 2017, Australia has actually passed the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 in December 2018 that does introduce such distinction. The act defines systemic vulnerability as well as systemic weakness as follows: "systemic vulnerability means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified." See https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_aspassed/toc_pdf/18204b01.pdf;fileType=application/pdf.

[25] For further discussion of proposed principles and modalities for striking a balance regarding law enforcement access to products and services, see Ian Levy and Crispin Robinson, "Principles for a More Informed Exceptional Access Debate," Lawfare, November 29, 2018, https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate; and Bruce Schneier, "Evaluating the GCHQ Exceptional Access Proposal," Lawfare, January 17, 2019, https://www.lawfareblog.com/evaluating-gchq-exceptional-access-proposal.

[26] These assume significance only if the intervention is of an ad hoc nature. Pervasive intrusion into the supply chain may well obviate the need for replication or propagation features. Deep persistency, in the sense of introducing deep into a system an external command and control function to monitor, exfiltrate, and/or manipulate it from afar, is a double-edged sword. It can help limit the damage the intervention inflicts but also has the potential to dramatically scale it up. Moreover, the discovery that such a mechanism has been introduced into ICT/OT systems would inevitably be cause for great concern.

[27] See, Bruce Schneier: "What Stuxnet looks for is a particular model of Programmable Logic Controller (PLC) made by Siemens (the press often refers to these as SCADA systems, which is technically incorrect)." From https://www.schneier.com/blog/archives/2010/10/stuxnet.html. An observation reinforced by this Siemens post: "Stuxnet infects Windows systems in its search for industrial control systems, often generically (but incorrectly) known as SCADA systems."

[28] This does not deny Stuxnet's long-term impact once the zero-day vulnerabilities that Stuxnet exploited were exposed (including reverse engineering and exploitation by others), or its broader strategic effects both on Iran and on cyberwarfare writ large.

[29] See Electronic Privacy Information Center, "Vulnerabilities Equities Process," https://epic.org/privacy/cybersecurity/vep/; Jason Healey, "The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers," *Columbia Journal of International Affairs*, November 2016, https://jia.sipa.columbia,edu/online-articles/healey_vulnerability_equities_process; and Ari Schwartz and Rob Knake, "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process," Belfer Center for Science and International Affairs, June 2016, http://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf; and Rob Joyce, "Improving and Making the Vulnerability Equities Process Transparent Is the Right Thing to Do," November 15, 2017, https://www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/ as well as "Vulnerabilities Equities Policy and Process for the United States Government" November 15, 2017, https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF. For further elaboration on this concept and our proposal for an international VEP norm, see Kate Charlet, Sasha Romanosky, and Bert Thompson, "It's Time for the International Community to Get Serious About Vulnerability Equities," Lawfare, November 15, 2017, https://www.lawfareblog.com/its-time-international-community-get-serious-about-vulnerability-equities.

[30] A *Wired* story describes the case in detail. See https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

31 One complication that must be taken into account here is that many (most?) vulnerabilities that one chooses to exploit give the attacker complete control over the target system. While a specific attack (including the part that exploits the vulnerability and the components that exfiltrate data, and so on) may be designed to attack confidentiality, it is easy to reverse engineer the attack, extract the core exploit, and use it for other purposes.

32 Which is to acknowledge that not only commercial considerations, but also cultural, ideological, and political factors could produce some variance in corporate proclivity toward entering such arrangements.

33 See Microsoft's Tech Accord (https://cybertechaccord.org/accord), Siemens' (and its allies) Charter of Trust (https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/corporate-core/topic-areas/digitalization/cybersecurity/shi-13378-cot-dok-narrative-online-2018-02-13-sbi-en.pdf), and the Open Group Trusted Technology Forum and the "Technology Provider Standard – Mitigating Maliciously Tainted and Counterfeit Products" it has produced. See (O-TTPS) V1.1.1 (September 2018) https://publications.opengroup.org/c185-1; see also, ISO/IEC 20243-1:2018, "Information Technology—Open Trusted Technology Provider™ Standard (O-TTPS)—Mitigating maliciously tainted and counterfeit products – Part 1: Requirements and recommendations" (2018) https://www.iso.org/standard/74399.html. Several other related initiatives under way are discussed on pages 14–27 of Huawei's June 2016 white paper, see Andy Purdy, "The Global Cyber Security Challenge," Huawei, June 2016, http://www-file.huawei.com/-/media/CORPORATE/PDF/white%20paper/The_Global_Cyber_Security_Supply_Chain_Security_June%202016_en.pdf?la=en&source=corp_comm.

34 One cannot exclude the possibility that some states would pass laws that require corporations cooperate with authorities that legally require intrusive access into their products, data, systems, or services. Some examples for such demands appear in notes 12–15, above. Such corporations could try to lobby against the passage of such laws (which many Western companies have done) and/or find cautious ways of making public the demands that are made to them under the law (or at least informing the affected parties). Corporations in some countries could challenge laws in the courts, and limit their collaboration to the narrowest legitimate interpretation of their obligation under the law. In extreme cases, when they would be legally required to introduce systemic vulnerabilities rather than ad hoc ones, they would be better off relocating their operations affected by such requirements to states that impose no such requirements.

35 Volkswagen Group's covert addition of software to defeat emissions standards inspection, and Uber's alleged use of Greyball to not only identify and deny services to problematic clients but also undermine law enforcement detection of their business practices, illustrate kinds of profit-motivated corporate activity that should be forsworn. See Alex Davies, "EPA: VW Cheated on Emissions Tests for 10,000 More Cars," *Wired*, November 2, 2015, https://www.wired.com/?p=1922167; Mike Isaac, "How Uber Deceives the Authorities Worldwide," *New York Times*, March 3, 2017, https://www.nytimes.com/2017/03/03/technology/uber-greyball-program-evade-authorities.html.

36 See, for instance, principles for software assurance including SAFECode's "Fundamental Practices for Secure Software Development," https://www.safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf; and NIST's "Software Assurance Metrics and Tool Evaluation," https://samate.nist.gov/Main_Page.html.

37 "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," NIST Special Publication 800-160, builds on ISO/IEC 15288 standard seems a useful complement especially for acquisition of governmental systems. See https://csrc.nist.gov/News/2016/NIST-Releases-SP-800-160-Sys-Security-Engineering.

38 See Nicole Perlroth, "How Antivirus Software Can Be Turned Into a Tool for Spying," *New York Times*, January 1, 2018, https://www.nytimes.com/2018/01/01/technology/kaspersky-lab-antivirus.html; Lily Hay Newman, "Inside the Unnerving Supply Chain Attack That Corrupted CCleaner," *Wired*, April 17, 2018, https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/.

39 For a high-level supply chain standard, see ISO/IEC 27036.

40 The "Coordinated Vulnerability Disclosure Manifesto" provides an instructive illustration of a private sector-led initiative to formulate best corporate practices in handling vulnerabilities research and disclosure and promote adherence to them. See https://www.thegfce.com/documents/publications/2016/05/11/responsible-disclosure-manifesto. There are various other ideas one may discuss in this context of corporate programs and practices designed to enhance the integrity of their products and services and to ascertain that they cannot be readily exploited as attack vectors. A more recent development of considerable importance in this domain is the public release by the U.S. CERT of a Guide to Coordinated Vulnerability Disclosure. See https://www.sei.cmu.edu/news-events/news/article.cfm?assetid=503398. Additionally, the 2018 version edition of ISO 29147 is focused on this issue as well, although it is not freely available.

41 An interesting test case for this norm would be the follow up to the May 2017 announcement by Intel of a critical vulnerability in its AMT manageability firmware that persisted for quite a few years. See https://www.intel.com/content/www/us/en/architecture-and-technology/intel-amt-vulnerability-announcement.html.

42 A case in point is Microsoft's white paper released at EWI's December 2014 Global Cyberspace Cooperation Summit in Berlin proposing six cybersecurity norms to limit conflict. The first of which called on states not "to target ICT companies to insert vulnerabilities (back doors) or take actions that would otherwise undermine public trust in products and services." See "Microsoft Launches White Paper on Global Cybersecurity Norms at Berlin Summit," EastWest Institute, December 15, 2014, https://www.eastwest.ngo/idea/microsoft-launches-white-paper-global-cybersecurity-norms-berlin-summit.

43 An important caveat here pertains to the scope of national laws (and related practices) defining necessary collaboration for vendors with the authorities. For example, Russian data localization and security laws, and other state behaviors, allegedly effectively weaponize Kaspersky as a vendor of cybersecurity products regardless of whether such development occurs with its knowledge and cooperation.

44 This requirement is inspired by a recent Australian statement that clarifies its requirements of prospective 5G suppliers. See https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers.

45 This composition was partially inspired by existing Charters of Trust such as those made public by CISCO (https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-trust-principles.pdf) and Siemens. Another useful document is Huawei's June 2016 white paper on "The Global Cyber Security Challenge," see http://www-file.huawei.com/-/media/CORPORATE/PDF/white%20paper/The_Global_Cyber_Security_Supply_Chain_Security_June%202016_en.pdf?la=en&source=corp_comm. However, the current undertaking goes much further than all of the existing documents, thanks to suggestions from and consultations with experts in industry, government, and think tanks around the world.

46 Article 19 of the USMCA articulates provisions pertaining to digital trade, and in 19.15 (2) calls for a risk-based approach for cybersecurity. It de facto incorporates the five functions of the NIST Cybersecurity Framework, namely identify, protect, detect, respond, and recover. Then Article 28 of the USMCA, which pertains to good regulatory practices, includes provisions to promote regulatory quality through transparency and accountability, inter alia by creating a committee to assist in countries' adherence to the principles.

[47] There are several clauses in the 2015 GGE report that refer to their recommendations of "norms, rules and principles for the responsible behaviour of States" that could be built upon in directions highlighted in this paper. None more so than article 13 (i) that says "states should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions." See http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174. Useful as the GGE platform might be, it is worth recalling, however, that the GGE report represents little more than governmental experts' recommendations. Moreover, the present language on supply chain allows flexible interpretations that many governments would likely find unconstraining.

[48] Interestingly, the Siemens Charter of Trust initiative seems to be moving in precisely both of these directions with regards to supply chain security. See https://new.siemens.com/global/en/company/topic-areas/digitalization/cybersecurity.html.

[49] Some of the most inspiring internationally respected multi-stakeholder initiatives that address key corporate social responsibility issues include the Voluntary Principles on Security and Human Rights (addressing the nexus of security and human rights for the extractive sector), the Fair Labor Association (addressing worker rights issues for the light manufacturing industry), the Global Network Initiative (addressing the protection of privacy and free expression by the information and communications technology sector), and the International Code of Conduct for Private Security Providers (addressing respect for human rights by private security providers), as well as the (now suspended) Nuclear Power Plant Exporters' Principles of Conduct. The most credible such initiatives maintain robust accountability mechanisms to ensure that the implementation of their standards of business conduct are effective. I am indebted to Gare Smith for information and guidance on assessing CSR processes and pointing out these examples.

[50] "ISM Principles of Sustainability and Social Responsibility With a Guide to Adoption and Implementation," Institute for Supply Management, https://www.instituteforsupplymanagement.org/files/About/526PrinSusSocRes_1_17.pdf.

[51] Both the Juniper Networks dual EC Incident (Stephen Checkoway et al, "A Systematic Analysis of the Juniper Dual EC Incident," https://dl.acm.org/citation.cfm?doid=2976749.2978395), and the discovery in 2017 of a serious hidden keylogger flaw in HP laptops (see http://www.bbc.com/news/technology-42309371) illustrate the difficulty of ascertaining which of these serious vulnerabilities have been created unintentionally and which have been part of an intentional design for corporate or other (national?) purposes.

[52] For detailed guidance on these and other supply chain security measures, see SAFECode's "Software Integrity Controls," https://www.safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf; and the Open Group's "Open Trusted Technology Provider Standard (O-TTPS)," https://publications.opengroup.org/c185-1.

[53] Here we must note that detection of vulnerabilities that are (or have been) in use is more likely than detection of vulnerabilities inserted for possible future use.

[54] Two instructive examples of such corporate transparency measures already in place come to mind here. One is the cooperation between the UK government and Huawei to establish a Huawei-funded government-cleared cell looking at hardware and software introduced into UK networks. The other is the Windows source code sharing by Microsoft with all governments that meet certain requirements.

[55] See endnote 48, above.

56 “Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace,” French Ministry of Europe and Foreign Affairs, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

57 “The Global Forum on Digital Security for Prosperity,” OECD, http://www.oecd.org/internet/global-forum-digital-security/.

58 “Developments in the Field of Information and Telecommunications in the Context of International Security,” UN Office for Disarmament Affairs, https://www.un.org/disarmament/ict-security.

59 I am most grateful to Bobbie Stempfley for drawing my attention to these issues.

60 These efforts include, notably, NIST’s Cyber Supply Chain Risk Management project (https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management) and the Open Group Trusted Technology Forum (http://www.opengroup.org/getinvolved/forums/trusted).

61 Which seems to be the direction advocated by the UK National Cyber Security Center with regard to 5G technology in general, and Huawei’s input into it in particular.

62 Peter Behner, Marie-Lyn Hecht, and Fabian Wahl, “Fighting Counterfeit Pharmaceuticals: New Defenses for an Underestimated – and Growing – Menace,” PwC, 2017, https://www.strategyand.pwc.com/media/file/Fighting-counterfeit-pharmaceuticals.pdf.

63 “Substandard and Falsified Medical Products,” World Health Organization, January 31, 2018, https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products.

64 Behner, Hecht, and Wahl, “Fighting Counterfeit Pharmaceuticals.”

65 “WHO Global Surveillance and Monitoring System for Substandard and Falsified Medical Products,” World Health Organization, 2017, https://www.who.int/medicines/regulation/ssffc/publications/GSMS_Report_layout.pdf?ua=1.

66 Ibid.

67 See, for instance, the blockchain application MediLedger, https://www.mediledger.com/. Kevin A. Clauson, Elizabeth A. Breeden, Cameron Davidson, and Timothy K. Mackey, “Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: An Exploration of Challenges and Opportunities in the Health Supply Chain,” Blockchain in Healthcare Today, March 23, 2018.

68 See the Pharmaceutical Security Institute, https://www.psi-inc.org/.

69 Harriet Agnew, “Sanofi Leads Charge Against Counterfeit Drugs,” *Financial Times*, December 3, 2017, https://www.ft.com/content/7027df4e-d67a-11e7-8c9a-d9c0a5c8d5c9.

70 Behner, Hecht, and Wahl, “Fighting Counterfeit Pharmaceuticals.”

71 U.S. Food and Drug Administration, “Drug Supply Chain Security Act (DSCSA),” September 21, 2018, https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa.

72 “WHO Global Surveillance and Monitoring System for Substandard and Falsified Medical Products,” World Health Organization.

73 Gaurvika M. L. Nayyar, et al., “Falsified and Substandard Drugs: Stopping the Pandemic,” *American Journal of Tropical Medicine and Hygiene* 100, no. 5 (2019), http://www.ajtmh.org/content/journals/10.4269/ajtmh.18-0981.

74 “Millions of Medicines Seized in Largest Operation Against Illicit Online Pharmacies,” EUROPOL, September 25, 2017, https://www.europol.europa.eu/newsroom/news/millions-of-medicines-seized-in-largest-operation-against-illicit-online-pharmacies.

75 International Federation of Pharmaceutical Manufacturers and Associations, https://www.ifpma.org/who-we-are/ifpma-in-brief/.

76 Alexander Gaffney, “FDA: Blockchain Could Be Used to Battle Counterfeiters, Secure Drug Supply Chain,” PwC, February 15, 2019, https://www.pwc.com/us/en/industries/health-industries/library/fda-says-blockchain-secure-drug-supply-chain-2-15-19.html.

77 Behner, Hecht, and Wahl, “Fighting Counterfeit Pharmaceuticals.”

78 A 2012 study by McKinsey found that adoption of a single global standard for healthcare products could achieve vast savings across the value chain—manufacturers, distributors, and providers—in addition to significant benefits for healthcare outcomes. See Thomas Ebel, et al., “Strength in Unity: The Promise of Global Standards in Healthcare,” McKinsey, October 2012.

79 “White Paper: The Need for Global Standards and Solutions to Combat Counterfeiting,” GS1 AISBL, 2013, https://www.gs1.org/docs/GS1_Anti-Counterfeiting_White_Paper.pdf.

80 GS1 standards for drug coding and identification are incorporated into national regulations in Europe and countries as diverse as Japan, Turkey, India, Argentina, and the United States. See “Discussion Paper on Medicines Identification Requirements on Primary Level Packaging Using GS1 Standards,” GS1, March 2019, https://www.gs1.org/docs/healthcare/position-papers/Discussion-paper-on-medicines-identification-requirements-on-primary-level-packaging-using-GS1-standards-final.pdf.

81 “WHO Global Surveillance and Monitoring System for Substandard and Falsified Medical Products,” World Health Organization.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org