The Next Pandemic Could Be Digital:

Open Source Hardware and New Vectors of National Cybersecurity Risk

Rick Switzer
February 2023

This paper was written by SCSP Senior Fellow Rick Switzer who is on a one-year sabbatical from the Department of State. Prior to joining SCSP, Rick was a State Department visiting professor at the National Intelligence University teaching graduate courses on China's economy and innovation system. Rick also served as a member of the Secretary of State's Policy Planning Council. From 2018 to 2019 he was a Senior State Department Advisor to the Department of Defense working with the Air Force and the Army. Preceding that he was the Environment, Science, Technology and Health Minister Counselor at Embassy Beijing, the largest science section in the world. Prior to joining government Rick co-founded a wireless technology start-up and also conducted innovation policy research at the University of California.

The views in this paper are the author's own and based on research he conducted prior to and during his sabbatical with SCSP. These views are not attributable to SCSP, the SCSP Board, or its staff.

Executive Summary

Open source technology is a powerful economic phenomenon that has unlocked economic value, but it also presents significant, yet poorly understood, challenges to national and economic security. Media and policy attention to date has focused on open source software: GitHub, for example, is an open source database where code is posted for all to use. Today, however, open source principles are being applied to computer hardware via initiatives like RISC-V (microprocessors); the Open Compute Project, or OCP (servers); and Open Radio Access Networks, or ORAN (networking equipment). If the current trajectory continues, it could lead to the commodification of the entire hardware stack, from microprocessors to server racks to routers, displacing today's industry leaders – the majority of which are headquartered in the United States or friendly nations.

With the rapid growth of the Internet of Things (IoT) and its application to critical infrastructure, widespread adoption of open source hardware (OSHW) and related standards risks creating new attack vectors for nation-state actors. 'Hardware trojans' allow cyber vulnerabilities to be inserted directly onto a chip or into a router. Even when vulnerabilities can be detected, the commodification of OSHW makes it increasingly difficult to trace a vulnerability back to its source. As the world's leading producer of lagging-edge microelectronics and 'white box' electronics,[1] the People's Republic of China (PRC) is best positioned to capitalize on these factors. Beijing has embraced OSHW as a disruptive offset, and PRC law requires firms to comply with the directives of the party-state.[2] *The PRC has both the means and the motive to weaponize the OSHW revolution*.

At present, the United States is not organized to prevent how the OSHW revolution could accelerate cyberattacks emanating from the hardware layer. OSHW is poorly understood outside technology circles, including within the U.S. Government, which lacks a coherent set of policies to address the national security challenges associated with OSHW. To defuse this threat, the United States must take rapid action. Sourcing from trusted suppliers – which I argue means restricting the use of core digital infrastructure components manufactured in countries of concern – is a key step to ensure that chips, circuit boards, and other hardware are not corrupted by malign actors. To implement this strategy, U.S. authorities should: 1) organize to respond to potential threats posed by OSHW produced in countries of concern, 2) develop robust security standards for OSHW, 3) increase disclosure requirements for U.S. firms, 4) consider blocking imports of OSHW from countries of concern, and 5) increase R&D funding for hardware-based cybersecurity.

[1] Henry Wai-chung Yeung, Executive Report, Global Production and Economic Development in Asia: A Study of Leading Electronics Firms and Their Production Networks, Global Production Networks Centre, National University of Singapore (2019).
[2] Nazak Nikakhtar, U.S. Businesses Must Navigate Significant Risk of Chinese Government Access to Their Data, Wiley (2021).

Future Scenario 2028

What began as a disruption of service from a series of regional banks has now expanded across the majority of the nation's cloud and internet router infrastructure, leading to severely limited internet access and an almost complete cessation of digital financial transactions. The original outages were initially traced to a service provider of cloud-based data storage and backend processing for regional banking and financial services firms, but outages now appear to be more widespread, covering close to 40 percent of all cloud-based data storage and processing services across the country. Just over a week after the crisis began, there are increasing reports of protests and looting of grocery stores where consumers encounter difficulties purchasing food due to the stores' inability to process non-cash transactions. Banks are similarly inundated with customers demanding to withdraw cash from their accounts to pay for daily necessities. Multiple agencies and private sector actors have scoured the affected data centers for the cause with most focused on cyber intrusion and offensive software-based cyberattacks.

Eventually the Defense Microelectronics Activity discovered the issue, identifying a hardwired, hardware-based on-off switch embedded in a series of voltage regulating chips that caused a chokepoint, preventing logic chips from connecting to the storage chips in the servers. Tracking the exact source of the affected chips has proven difficult, as virtually all of the affected hardware are commodity microelectronics components based upon open hardware standards that are sourced from the cheapest available supplier; however, virtually all are from hundreds of factories dispersed across China. Initial estimates show it will take 12-18 months to identify, remove, and replace all the corrupted hardware. However, as the only source for these commodity components are the same factories where they were originally procured, it is unclear if this strategy is feasible. The total economic cost of the crisis is expected to exceed trillions of dollars in damages and lost GDP, putting tens of millions of Americans out of work, and leading to unprecedented social unrest.

Overview

Open source software, an early vanguard of the open source phenomenon, has been revolutionary and disruptive.[3] Though largely developed in the United States and other democratic countries, the surge in open source software left many traditional U.S. technology firms facing challenges to their competitiveness. Other firms, however, have thrived on open source-based models, which are now used by the vast majority of companies. Products of the open source revolution include Linux, the software running most data centers around the world, and Android, the most popular smartphone platform globally. Now it is *hardware* that is being disrupted by the open source phenomenon.

Open source hardware is computer hardware – semiconductors, routers, servers, IoT devices, etc. – that features a design made publicly available that anyone can freely study, modify, distribute, make or sell the design or product. Given that all players are free to use OSHW equally, some might note, why should this be of concern to the United States Government, or any government for that matter? Put simply, OSHW is the future – and as will be demonstrated later in this paper, its rapid adoption has the potential to be massively disruptive.

OSHW could lead to the commodification of hardware and drive down costs for the world's largest software, networking, and internet platform companies. As with other transformational technology trends, many current market leaders are likely to face disruption or significant challenges to their business model. This will be particularly true for firms across the legacy hardware manufacturing industry which lack government subsidies to compete in a profit-constrained environment, a category that includes most U.S.-headquartered firms.

Three major OSHW initiatives currently dominate the space: RISC-V, an open source architecture for microprocessors; the Open Compute Project (OCP), a collective of hyperscalers working to bring open source hardware to the data center; and open network architectures, particularly Open Radio Access Network (ORAN) technology, which will apply open source standards to hardware for advanced networks. Taken together, these efforts cover most of the digital communications and technology landscape. Moreover, key industry leaders have embraced RISC-V, OCP, and ORAN,[4] and each initiative has been widely promoted with products making significant progress gaining market share.[5] RISC-V and other OSHW standards are being adopted rapidly, positioning them as potential de facto standards for global digital architectures.[6]

---

[3] Where not otherwise noted, the analysis presented is based on the author's conversations, site visits, and other firsthand observations over the course of hundreds of meetings between 2000 and 2022 with government officials (including at the Department of Commerce, Department of Defense, National Security Council, National Science Foundation, et al.), industry associations, academics, and technology companies ranging from startups to large multinationals in the United States, China, and elsewhere.

[4] Key industry leaders include, for example, Intel, Microsoft, Huawei, and Qualcomm.

[5] Semico Research's New Report Predicts There Will Be 25 Billion RISC-V-Based AI SoCs By 2027, RISC-V (2022); Wylie Wong, Open Compute Project Hardware Sales to Hit $46B by 2025, DataCenter Knowledge (2021); Open RAN Will Have 15% RAN Market Share by 2026 – Report, RC Wireless News (2022).

[6] RISC-V to Impact Communications Segment Reaching a 209% CAGR by 2025, Says Semico Research, Semico Research (2019); Alan Chang, The First 10 Years of the Open Compute Project – What It's Done and Where It's Going, DataCenter Knowledge (2022).

Much of Industry is All In on OSHW

OSHW is quickly expanding its market share across the technology industry, particularly the microelectronics and information and communications industries. Traditionally, a small number of key industry players primarily from the United States, Korea, Japan, and Europe – such as ARM and Intel – have designed and built the foundational integrated circuits that power these integrated systems. These private firms tightly controlled access to root-level cybersecurity and runtime authentication and protection capabilities that protected these chips and the systems they power from cyberattacks. Opaque by design, firms relied on potential adversaries' lack of knowledge about the source code and how the hardwired structure of these chips functioned, which provided a first line of defense against cyberattacks designed to surreptitiously control and/or destroy these networks.

The confluence of paradigm-shifting industry trends centered around open source hardware initiatives is transforming the business models for many leading information and communications technology (ICT) infrastructure companies, whether they realize it or not. Industry-led open source projects are positioned to become de facto standards for all digital infrastructure, concentrating competition into service provision versus branded cyber-infrastructure manufacturing. The implications for national security are profound.

Unlike software-based cyber vulnerabilities which can be addressed with a software patch and resolved across the entire network almost immediately, hardware vulnerabilities embedded in the physical structure of the chips and circuit boards cannot typically be resolved via software updates and instead require expensive and time-consuming hardware-based solutions. Industry leaders are looking to embed hardware-based security into their open source servers; however, ensuring that network architecture hardware is not corrupted requires **sourcing from trusted suppliers.**

OSHW's disruptive potential, with major implications for the global technology competition, requires more analysis and debate about the implications of this industry-driven phenomenon and the appropriate steps to address the risks it poses to national security. Beijing is organizing to dominate the OSHW movement, which it views both as a potential economic boon for the PRC's national technology goals and as a way to make itself immune to future U.S. export controls, since open source technologies are generally outside the scope of such restrictions.[7] This creates a new national security vulnerability for the United States and its allies and partners. Moreover, China already dominates 'commoditized' manufacturing for hardware, such as routers and laptops, and OSHW enables China to obtain or forgo IP in critical sectors where it is not yet dominant, without having to invest in R&D.[8] Beijing's Made in China 2025 plan and Dual Circulation Strategy make clear that the PRC plans to dominate every aspect of the global electronics supply chain. Additionally, the PRC's state planners have already embraced OSHW as an alternative to western-dominated portions of the electronics industry. According to Professor Henry Yeung of the National University of Singapore, China currently accounts for 30 to 32

[7] Karen M. Sutter, China's New Semiconductor Policies: Issues for Congress, Congressional Research Service (2021); Ann Cao, Tech War: China Bets on RISC-V Chips to Escape the Shackles of U.S. Tech Export Restrictions, South China Morning Post (2022).
[8] These critical sectors include, for example, servers, application-specific integrated circuit (ASICS) chips, CPUs, GPUs, and field-programmable gate arrays (FPGAs).

percent of global electronics manufacturing.[9] Given these factors, the OSHW trend could force current industry leaders – many of which are western firms – to either source production from PRC factories or pivot to a service provider model, thereby exiting the electronics hardware manufacturing business. The manufacturing of hardware components for emerging electronics technologies such as IoT are already dominated by factories in China and Taiwan, many of which produce for western firms. Under an OSHW regime, PRC dominance could be further solidified.

The Open Source Hardware Ecosystem, Explained

RISC-V and OCP are Stealth Standards: Stealth technology standards can be defined as a deeply integrated set of architectures, increasingly used by industry, that lock-in as de facto tech standards by virtue of their existence – irrespective of their perception as such by regulators. OCP initiatives include server designs, data storage, rack designs, energy efficient data centers, open networking switches, AI accelerator designs and, with the addition of the Open Domain-Specific Architecture (ODSA), OCP now includes open microchip design for systems on chips (SOCs) and FPGA-bases solutions. Additionally, RISC-V is increasingly expanding into major categories of semiconductors including CPUs, GPUs, FPGAs, and many more.

In the broadest sense, a technology standard is a set of rules, processes, or structures designed to provide interoperability through agreed-upon planning, development, operation, and governance mechanisms. By this definition, OCP and RISC-V are clearly technology standards. However, these open source hardware standards are little understood by many governments, with the exception of the PRC, and do not receive the same attention and official participation as major international standards bodies, including at 5G/3GPP, IEEE, ISO, and MPEG. As these technologies' market penetration increases, they are well-positioned to become *the* standard that runs core digital infrastructure and, as such, require governmental participation commensurate with their growing importance.

1. What Is RISC-V?

RISC-V combines a modular technical approach with an open license business model, meaning that anyone, anywhere, can leverage the IP contributed and produced by RISC-V International.[10] RISC-V has broken down barriers in the semiconductor industry, bringing together different companies, industries, and geographies for open collaboration. The RISC-V Foundation was established in 2015 with the Chinese Academy of Sciences and U.S.-based multinational firms like Google and IBM among its founding members.[11] As the organization's website notes, "RISC-V does not take a political position on behalf of any geography. We are proud to see organizations from around the world working together in this new era of processor innovation."[12] According to RISC-V

[9] Henry Wai-chung Yeung, Executive Report, Global Production and Economic Development in Asia: A Study of Leading Electronics Firms and Their Production Networks, Global Production Networks Centre, National University of Singapore (2019).
[10] Note: Originally conceived at UC Berkeley in 2010, RISC-V built upon DARPA- and NSF-funded foundational research at Berkeley in 1981. See Milestones: First RISC (Reduced Instruction Set Computing) Microprocessor 1980-1982, ETHW (last accessed 2022). The Bayh-Dole Act passed in 1980 ensured that the U.S. Government-funded research remained the intellectual property of Berkeley. See Bayh-Dole Act, 35 U.S.C. § 200 (1980).
[11] Scott Foster, Open-Source IC Architecture Taking Off in China, Asia Times (2022).
[12] About RISC-V, RISC-V (last accessed 2023).

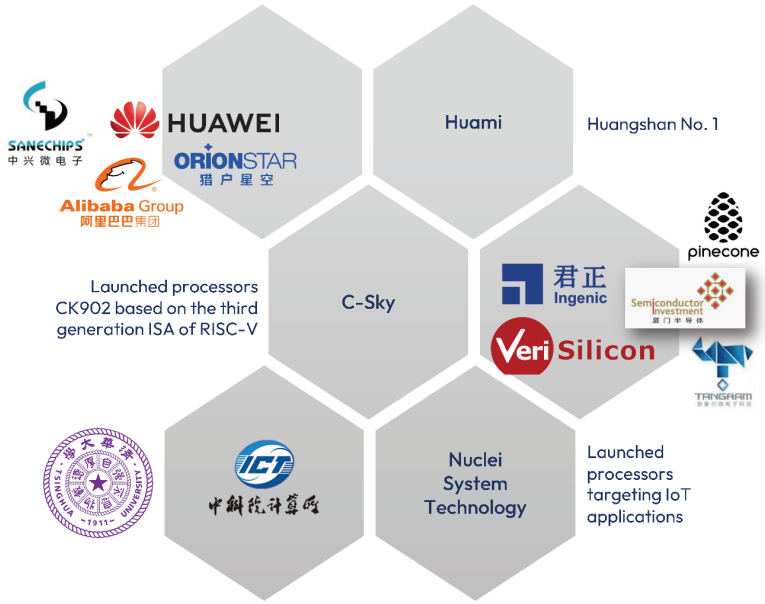
Foundation's CEO, Calista Redmond, the organization moved its headquarters from the United States to Switzerland to ensure that members, which include Huawei and Alibaba, would not be subject to U.S. technology transfer restrictions.[13]

At the current rate of adoption, RISC-V will soon stand alone as the standard for universal instruction set architecture (ISA) for small IoT devices, personal mobile devices, industrial controllers,[14] and warehouse-level computers – potentially within the next five years.[15] Several leading firms have begun production in China of RISC-V chips for various applications – SiFive is creating SSD Controllers,[16] while Alibaba and Xilinx are finalizing designs for cloud and FPGA systems, respectively.[17] Shanghai-headquartered StarFive is producing RISC-V-based CPUs designed to replace ARM's technology in computing, data centers, telecommunications equipment, and industrial applications.[18]

The PRC View: The Chinese government sees OSHW as important to its quest to reduce its technology dependency on the United States and other countries.[19] Having anticipated the United States' ability to restrict PRC companies' access to proprietary chips produced by non-Chinese companies, the government helped found the "China RISC-V Alliance," which aims to increase the development and adoption of open source architecture in China and reduce reliance on Western-controlled x86 and ARM architectures.[20] The first resulting special-purpose chips are already in production by Chinese companies. Beyond circumventing U.S. export control regimes and leapfrogging ahead in semiconductor design, Beijing's interests may also stem from a desire to access and embed cybersecurity flaws at the design phase. The open nature of RISC-V's instruction-set architecture (ISA) provides adversaries with architectural details and information on system security vulnerabilities that offer greater opportunity for exploitation.[21]

[13] Nitin Dahad, RISC-V to Move HQ to Switzerland Amid Trade War Concerns, EETimes (2019).
[14] Ensuring the Success of Your RISC-V Product with a Commercial-Grade Software Development Ecosystem, Siemens (last accessed 2023).
[15] Tao Lu, A Survey on RISC-V Security: Hardware and Architecture, arXiv (2021).
[16] SiFive Storage Solutions: How RISC-V and Custom Silicon Platforms Enable Smart Storage Architectures, SiFive (2020).
[17] Chen Chen, et al., Xuantie-910: Innovating Cloud and Edge Computing by RISC-V, IEEE (2020); Yipeng Zhang, et al., Parallel DNN Inference Framework Leveraging a Compact RISC-V ISA-Based Multi-Core System, Association for Computing Machinery (2020).
[18] Scott Foster, Open-Source IC Architecture Taking Off in China, Asia Times (2022).
[19] Anna Gross & Qianer Liu, China Enlists Alibaba and Tencent in Fight Against US Chip Sanctions, Financial Times (2022); China's New Semiconductor Policies: Issues for Congress, Congressional Research Services at 5, 7 (2021).
[20] Anna Gross & Qianer Liu, China Enlists Alibaba and Tencent in Fight Against US Chip Sanctions, Financial Times (2022).
[21] Tao Lu, A Survey on RISC-V Security: Hardware and Architecture, arXiv (2021).

China's RISC-V Ecosystem



22

2. What Is the Open Compute Project (OCP)?

OCP was launched in 2011 by Facebook and a group of U.S. companies including Intel, Goldman Sachs, and Rackspace.[23] Similar to the open source software initiatives, OCP seeks to break the ownership of intellectual property that drives market share and industry control of legacy U.S. industry players over cloud and router hardware. According to industry estimates, OCP gear represented about 25 percent of the 11.7 million server shipments in 2019,[24] with the majority coming from OCP board members Facebook and Microsoft.[25] According to a study commissioned by Inspur, Beijing's national champion in the server industry, OCP and related open standards will account for 40 percent of servers shipped globally by 2025.[26]

OCP are the Servers of Choice for 5G Telecommunications Firms: In 2019, AT&T released a detailed specification for a cell site white box gateway router based upon OCP's open-router design.[27] This white box blueprint is a reference design that any hardware manufacturer can use as a guide to build these routers. Since then, AT&T announced its

[22] Companies and entities in China which support RISC-V — partial list. See Why RISC-V Lags in China, EETimes (2018) (citing VeriSilicon).
[23] Note: Open Compute Project (OCP) is creating an entire server, storage, and data management ecosystem based upon open source designs and code meant to drive costs out of the hardware business by commoditizing the entire infrastructure. Facebook Launches Open Compute Project, Meta (2011); About, Open Compute Project (last accessed 2023).
[24] Server Shipments Worldwide from 2010 to 2020, Statista (2022).
[25] Alan Chang, The First 10 Years of the Open Compute Project – What It's Done and Where It's Going, DataCenter Knowledge (2022).
[26] Vladimir Galabov, Open Computing Is for Everyone and Is Here to Stay, Omdia at 9 (2021).
[27] AT&T Submits Design for Service Provider-Class Routers to the Open Compute Project, AT&T (2019).

plans to install more than 60,000 open source, software-powered white boxes across its network in support of its 5G plans – AT&T estimates that it will need 250,000 to 300,000 of these routers to meet its U.S.-based 5G network demands[28] – accounting for 25 percent of the total needed.[29] Commodity producers from Taiwan and China currently produce all of these white-box routers. These routers will eventually form the infrastructure that could enable not just phones and tablets to connect to its mobile 5G network, but also new technologies like autonomous vehicles, drones, augmented reality and virtual reality systems, smart factories, and more. Major telecommunications service providers like AT&T have embraced OCP and other open hardware initiatives and are expected to invest billions in open source hardware to support 5G rollout. AT&T outlined plans to virtualize more than 75 percent of its network functions by 2020, thanks to a new model featuring sophisticated software running on commodity hardware.[30] The company's plans call for AT&T to become a software and networking company, transforming the storied telecommunications infrastructure company into a virtual network service provider.

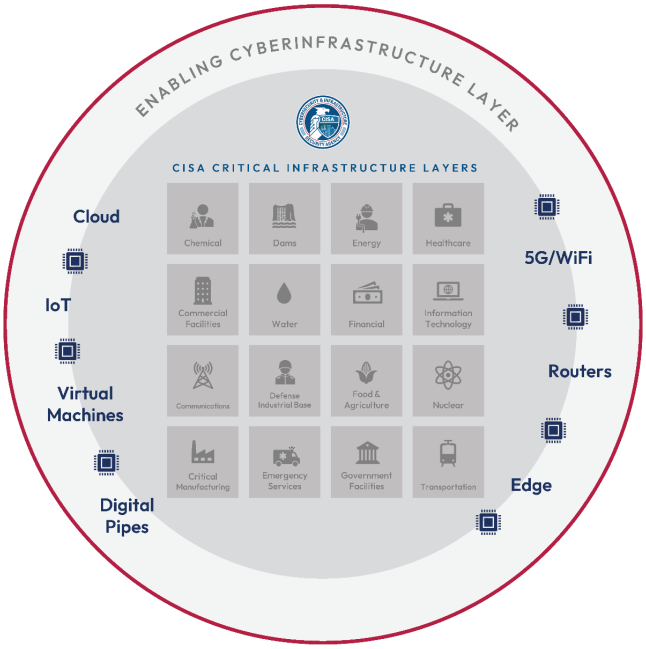
OCP Network Security: Many open source industry advocates maintain that OCP architecture can be made just as secure as traditional proprietary servers.[31] In order to address the inherent vulnerabilities of a source code that is open to all – a problem not faced by incumbents, like Cisco in routers and IBM in servers, whose source code remains a trade secret – Microsoft and Google have developed chip-based hardware solutions that can prevent unauthorized access to servers and routers based upon OCP designs. This suggests that large technology players are aware of the security threat OSHW poses. Microsoft's Cerberus chip prevents alterations to the source code of the servers' hardware by authenticating the hardware at the circuit-board level.[32] The need for dedicated hardware like the Cerberus chip indicates the seriousness of the cybersecurity challenge that even world-class technology firms now face, including both external software-based attacks and hardwired vulnerabilities such as hardware trojans. An analytical review of the current literature and the author's judgment based upon firsthand observations strongly suggests that sourcing from trusted suppliers is a key step toward ensuring that chips and circuit boards are not corrupted by malign actors at the hardware level before installation.[33] While no single step is sufficient to ensure that hardware is completely secure – as numerous accidental flaws and vulnerabilities can expose systems to external attacks – closing the primary attack vector from countries of concern is a critical step.

In 2012, soon after the launch of OCP, China's Academy of Information and Communication Technology – which falls under China's Ministry Industry and Information Technology – consulted with Intel, then joined with Alibaba, Baidu, Tencent, China

[28] Stephen McBride, This Stock Is America's 5G 'Landlord', And It Pays A 3.8% Dividend, Forbes (2019).
[29] AT&T Is Deploying White Box Hardware in Cell Towers to Power Mobile 5G Era, AT&T (2018).
[30] AT&T is Deploying White Box Hardware in Cell Towers to Power Mobile 5G Era, AT&T (2018). AT&T achieved this goal in 2020 and has since announced plans to move its 5G network to Microsoft's Azure cloud service. Martin Perlin, AT&T, the Pandemic and a Disaggregated Core Router, DriveNets (2020); AT&T Moves 5G Mobile Network to Microsoft Cloud, AT&T (2021).
[31] Based on author discussions with industry experts, OCP leadership, and academia.
[32] Project Cerberus, Microsoft (2022).
[33] Author assessment based upon interviews with hundreds of cybersecurity specialists, researchers, government officials, technology firms, and industry groups in China and the United States between 2000 - 2022.

Telecom, and China Mobile to form the Open Data Center Committee (ODCC), China's version of OCP.[34] ODCC is structured around six working groups: the Data Center Server, Data Center Infrastructure, Data Center Network, Edge Computing, Intelligence Monitoring and Management, and New Technology and Test.[35] In a 2019 press release, PRC technology giant Baidu announced "a new collaboration with Facebook and Microsoft to define the OCP Accelerator Module (OAM) specification to increase the adoption of artificial intelligence (AI) accelerators to benefit the development of AI. The OAM specification, which is expected to shorten the development of AI accelerators and speed up large scale adoption, is led by Baidu, Facebook, and Microsoft, and supported by leading internet companies, AI accelerators leaders, AI accelerators startups, as well as ODM/OEMs."[36]

Semiconductors Power Entire Ecosystems



[37]

The new open source hardware paradigm presents a cybersecurity threat vector for which we are unprepared.

[34] Introducing the Open Data Hub Council, Open Data Center Committee (last accessed 2022). According to MIIT's website, MIIT is responsible for "new-type industrialization development strategies and policies, coordinate and solve major problems in the process of new-type industrialization, formulate and organize the implementation of development plans for industry, communications, and informatization, promote strategic adjustment, optimization and upgrading of industrial structures, and promote informatization and the integration of industrialization that promotes the construction of a military-civilian combination and military-in-civilian weaponry research and production system." (Emphasis added). See 2022 Departmental Budget of the Ministry of Industry and Information Technology, Ministry of Industry and Information Technology (2022).
[35] Open Data Center Committee Structure (last accessed 2023).
[36] Dirk Van Slyke, Baidu, Facebook, and Microsoft Work Together to Define the OCP Accelerator Module Specification, Open Compute Project (2019).
[37] Critical Infrastructure Sectors, U.S. Cybersecurity & Infrastructure Security Agency (last accessed 2023).

3. What Is Open Radio Access Network (ORAN) Technology?

The radio access network (RAN) is the final wireless link between a network and a mobile device. The RAN contains the radio unit, the distributed unit, and the centralized unit that form the core network (Core) which controls the 5G telecommunications network. ORAN is an industry-led open source hardware initiative that seeks to disaggregate RAN functionality with a mix of industry-defined, proprietary and open interface specifications between these constituent elements. It can be implemented in vendor-neutral hardware and software-defined technology based upon open interfaces and community-developed standards. Open interfaces include (open) fronthaul and (open) midhaul, connecting the different parts of the RAN and (open) backhaul between the RAN and the Core. In practice, **this allows a network to be built and customized with components from multiple vendors.** This is a major shift from current network architectures in which a single telecom operator uses only its proprietary combination of hardware and software in the RAN stack, and thus is responsible for its integration and end-to-end security. Proponents of ORAN argue that it could reduce costs, increase innovation, and even make it easier for U.S. firms to reenter the telecom infrastructure market. If components are sourced from trusted suppliers in jurisdictions bounded by the rule of law and an independent judiciary, and integrated and managed properly, ORAN does not necessarily pose an increased cybersecurity risk. It can, however, increase network complexity, raising risks for unsophisticated users.

Beijing is also working to shape ORAN standards. The PRC's OTII Open Telecom IT Infrastructure, affiliated with ODCC, was launched in November 2017 by China Mobile, China Telecom, China Unicom, China Telecom, and Intel. OTII's primary goal is to build and optimize open standards and unified server solutions and products for 5G and telecommunications-focused edge computing.[38] According to a 2019 study funded by Inspur, OTII server specs were adopted by the PRC as the recommended open solution for ORAN.[39]

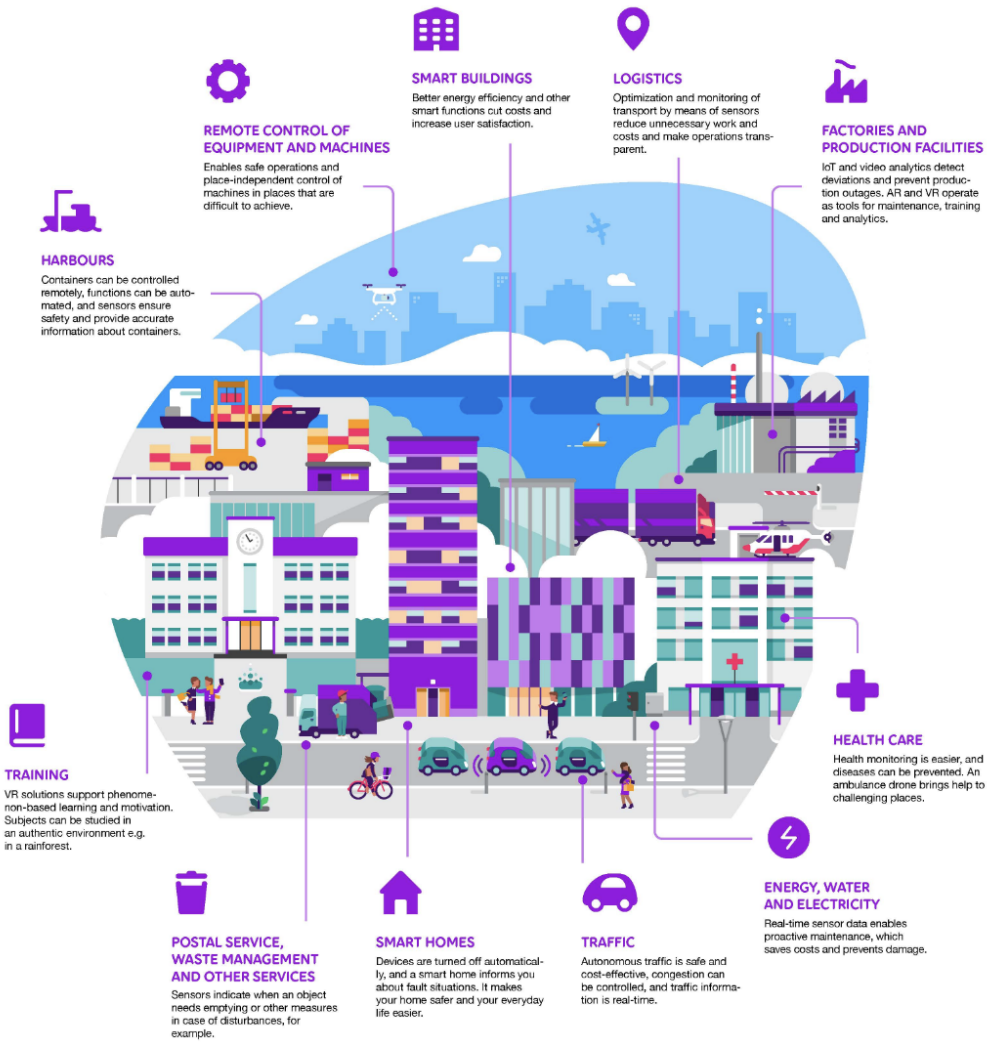
Digital Infrastructure Orders Our Lives

The open source revolution is occurring in parallel with the ongoing revolution in cloud computing, edge computing, and IoT, which is embedding a matrix of low latency, always-on smart devices throughout our societies. According to the International Data Corporation, nearly 42 billion IoT devices could be deployed by 2025.[40] These devices not only create seamless communications and data-centric utilities, but they also directly impact the physical world by creating what are known as cyber-physical systems (CPS). Embedded processors and processor engines that were previously powered by proprietary cores from UK-based ARM Holdings are now increasingly powered by open and free architectures like RISC-V.[41] These networks of

[38] OTTI Server Technical Specification, Open Data Center Committee at 2 (2019).
[39] Vladimir Galabov, Open Computing Is for Everyone and Is Here to Stay, Omdia at 7 (2021).
[40] Internet of Things and Data Placement, Dell Technologies (last accessed 2022) (citing Carrie MacGillivray & David Reinsel, Worldwide Global DataSphere IoT Device and Data Forecast, 2021–2025, IDC (2019).
[41] Alasdair Armstrong, et al., ISA Semantics for ARMv8-a, RISC-V, and CHERI-MIPS, Proceedings of the ACM on Programming Languages (2019).

devices touch every aspect of modern life from factories, logistics centers, electrical grids, and water systems to hospitals, traffic systems, smart homes, and government services.

The core cyber systems upon which our national security, modern economy, and increasingly all aspects of human existence depend are run and controlled by trillions of embedded semiconductors. This critical hardware and the integrated circuits (ICs) that power them depend on embedded, hardwired cyber security cores to enable trust and create the environment that allows software-based cybersecurity to function. But software-based cybersecurity can be undercut if vulnerabilities are inserted directly into the hardware.



Telia 42

[42] 5G Finland, Telia (last accessed 2023).

The Hardware Threat: Cyber Vulnerabilities Hardwired into the Ecosystem

Ultimately, the OSHW model raises serious cybersecurity concerns. Network security researchers have discovered numerous backdoors in Chinese telecom equipment (such as those made by Huawei and ZTE), and security agencies have subsequently been forced to introduce software patches and other safeguards.[43] The threat of state-backed attackers, who may use advanced techniques to tap into backdoors in routers manufactured by any producer worldwide,[44] is problematic for data security; however, OCP and other open source hardware standards potentially present an even more dire scenario – surreptitious control or denial of service on a nation-wide scale.

Unlike traditional cybersecurity vulnerabilities stemming from software, OSHW creates new attack vectors that are more difficult to resolve. These are several reasons for this. First, security at the root level becomes very difficult to manage as the risk of hardware trojans built into components grows exponentially.[45] This decentralization also leaves overall cybersecurity responsibility diffuse, as industry players no longer carry responsibility for ensuring their products remain secure. Moreover, the commoditized nature of OSHW leaves the original sources of production obscure, creating new supply chain risks by rendering it difficult if not impossible to determine whether a piece of hardware was produced in Mexico or China. If left fully unexamined and unregulated, the United States could find its entire cyber-physical infrastructure compromised and dependent on an adversarial power.

Hardware Trojans

Hardware vulnerabilities originate either from error or from intentional insertion of malicious errors.[46] While unintentional flaws and runtime errors can lead to major cybersecurity vulnerabilities, in some cases they can be mitigated after the fact. Hardware trojans are the malicious modification of hardware during design or fabrication.[47] For example, a recent vulnerability discovered in Siemens S7-1500 industrial controllers involved a flaw in the firmware of the controllers.[48] The company's product security advisory notes: "Affected devices do not contain an Immutable Root of Trust in Hardware. With this the integrity of the code executed on the device can not be validated during load-time. An attacker with physical access to the device could use this to replace the boot image of the device and execute arbitrary code."[49] Siemens has no plan to fix the issue and plans to allow the products to be slowly phased out over time. According to a third-party analysis, "the vulnerability stems from a basic error in how the cryptography is implemented, but Siemens can't fix it through a software patch because the scheme is physically burned onto a dedicated ATECC CryptoAuthentication chip."[50] While all indications suggest that this flaw was an unintentional error added during the design or

[43] Bernard Meyer, Walmart-Exclusive Router and Others Sold on Amazon & Ebay Contain Hidden Backdoors to Control Devices, Cybernews (2022).
[44] Same Cloak, More Dagger: Decoding How the People's Republic of China (PRC) Uses Cyber Attacks, Booz Allen Hamilton (2022).
[45] Rajat Subhra Chakraborty, et al., Hardware Trojan: Threats and Emerging Solutions, IEEE (2009).
[46] Mohammad Rahmani Fadiheh, et al., Processor Hardware Security Vulnerabilities and Their Detection by Unique Program Execution Checking, IEEE (2019).
[47] Rajat Subhra Chakraborty, et al., Hardware Trojan: Threats and Emerging Solutions, IEEE (2009).
[48] Note: Firmware is the low-level code that coordinates hardware and software on a computer.
[49] See Siemens Product Advisory Note, SSA-482757: Missing Immutable Root of Trust in S7-1500 CPU devices, Siemens (2023).
[50] Lily Hay Newman, A Widespread Logic Controller Flaw Raises the Specter of Stuxnet, Wired (2023).

fabrication process, it clearly demonstrates that hardwired and/or root-level firmware errors, whether added by design or human error, are often impossible to fix after the fact and require either living with the new vulnerability or undertaking a very expensive 'rip and replace' project.

Hardware-level vulnerabilities are not an isolated issue. According to a recent study by Aachen University's Institute for Communications Technologies and Embedded Systems, "malicious circuit modifications known as hardware trojans represent a rising threat to the integrated circuit supply chain."[51] The paper further notes that outsourcing of production to untrusted foundries has given rise to hardware trojans, concluding that these modifications can lead to denial of service attacks, data theft, circuit alteration, and more. The paper proposes a solution that would require the designer to be outside the malign circle seeking to embed the trojan. However, many RISC-V and other chips embedded into OCP and other systems, such as servers from PRC national champion Inspur, will be designed and fabricated by PRC firms subject to control by state security services. I have not discovered in my research any proposed schema for hardware trojan mitigation that acknowledges, much less addresses, threats from nation-state cyber-intrusion and control strategies emanating from countries of concern where the chips are fabricated, rather than from malign actors acting independently.

When intentionally embedded on a chip or electronics component, hardware trojans can cause irreparable damage to critical systems. If not discovered before tape-out and fabrication, there are few if any ways to mitigate the vulnerability; firmware and software updates will not clear the chips's hardware runtime behavior and could require a complete rip and system replacement.[52] Industry remains behind on developing tools and mechanisms to prevent dangerous hardware trojans. This issue is further compounded by an assumption of trust in the partner firm producing the component, even when partner firms are located in countries of concern.[53]

PRC experts are well aware of the threat posed by hardware trojans. A recent People's Liberation Army study, published by the Institute of Electronics, Information and Communications, noted that "hardware trojans is (sic) one of the main threats to security, especially attacks on General-Purpose Registers (GPRs) of processors."[54] The study also noted that other mitigation studies often require complex computation and cannot detect a HWT induced attack on GPRs in real time.

Systemic Cloud and Telecommunications Vulnerabilities

IoT will link tens of billions of devices to the cloud, the edge, and to other devices, controlling vehicles, unmanned aerial vehicles, medical devices, smart grids, industrial robots and sensors, and much more. Industry predicts there will be close to 42 billion connected IoT devices by 2025,

[51] Dominik Šišejković, et al., Control-Lock: Securing Processor Cores Against Software-Controlled Hardware Trojans, Institute for Communications Technologies and Embedded Systems (2019).
[52] Tao Lu, A Survey on RISC-V Security: Hardware and Architecture, arXiv (2021).
[53] See Alexander Hepp, et al., A Pragmatic Methodology for Blind Hardware Trojan Insertion in Finalized Layouts, arXiv (2022).
[54] ShiWei Yuan, et al., Real-time Detection of Hardware Trojan Attacks on General-Purpose Registers in a RISC-V Processor, IEICE Electronics Express (2021).

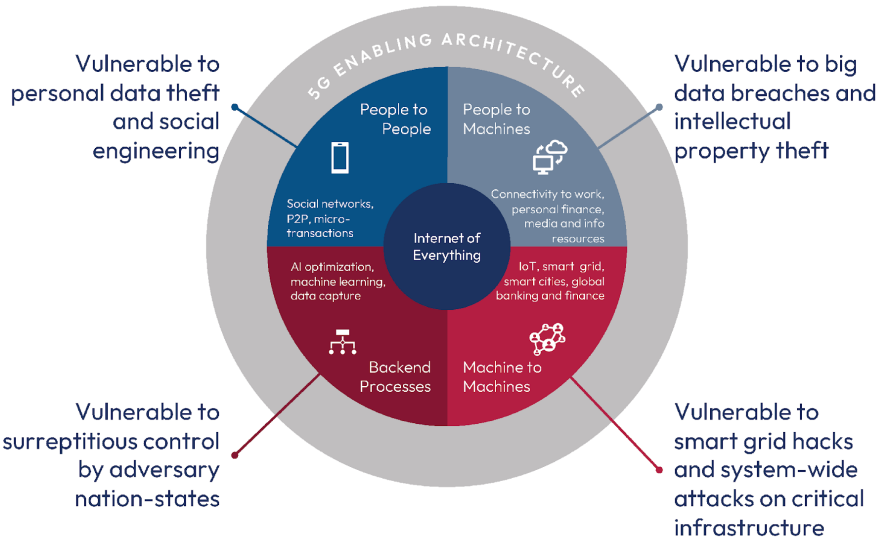
creating more than 79 zettabytes of data.[55] All of this will take place without human intervention or oversight, creating vulnerabilities not present in previous technology paradigms. Denial-of-service attacks at the root level could cripple the entire critical and defense infrastructure of countries using unsecure hardware.

Industrial Manufacturing 4.0

Industrial manufacturing 4.0 builds on the power of the Industrial IoT (IIoT). At its core are cyber-physical systems – smart, autonomous systems that use computer-based algorithms to implement a matrix of sensors, servos, and automated AI-driven processes to monitor and control physical things like energy infrastructure, machinery, robots, and vehicles.[56] Industry 4.0 is rapidly expanding across the industrial landscape, creating enormous increases in productivity; however, systemic risks are not well understood, creating vulnerabilities across the entire production base.[57] The primary vectors for cyberattacks on CPS industrial networks are side-channel attacks, where information is exfiltrated via peripheral systems; direct sabotage, where defects or runtime errors are introduced into the supply chain or cloud storage; reverse engineering, where attackers are able to reproduce the exact component which is being produced (an issue of particular concern to the defense industrial base); and counterfeit production, which undermines IP and investment by original manufacturers.[58] Virtually all of these systems are being built on open source hardware and open source software standards. Moreover, the IoT and IIoT components that power the open source hardware and software are largely sourced from the lowest cost suppliers – typically, these are located in the PRC. Unlike Intel and AMD, which build in hardwired isolation security systems for CPUs, IoT devices have low power and limited resources, which complicates the use of resource-intensive security schemas.[59]

[55] Sam George, IoT Signals Report: IoT's Promise Will Be Unlocked by Addressing Skills Shortage, Complexity and Security, Microsoft (2019).
[56] Abroon Qazi & Barbara Gaudenzi, Supply Chain Risk Management: Creating an Agenda for Future Research, International Journal of Supply Chain Operations Resilience (2016).
[57] Nikhil Gupta, et al., Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks, IEEE (2020).
[58] Nikhil Gupta, et al., Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks, IEEE (2020).
[59] Sandro Pinto & Nuno Santos, Demystifying Arm TrustZone: A Comprehensive Survey, Association for Computing Machinery (2019).

The Internet of Everything



The PRC's Approach to Open Source

In April 2020, the PRC's National Development and Reform Commission (NDRC) and Cyberspace Affairs Commission (CAC) highlighted the importance of open source communities for industrial digitalization in an Implementation Plan for Digital Economy Development in the 14th Five-Year Plan[60] (2021-2025). NDRC further encouraged the development of open source algorithms in its March 2021 AI Innovation Work Plan[61].

OCP Helping to Fill Beijing's Technology Gaps: According to industry sources, OCP's AI accelerator project, developed by Facebook, Baidu, and Microsoft, is poised to power the backend AI servers underpinning all three companies' AI initiatives in the near future. Baidu and other PRC tech companies are behind on the design of AI-optimized server architectures and could benefit greatly from partnering with the OCP. While current designs remain highly dependent upon U.S.-based NVIDIA's GPUs to power computationally-intensive machine learning algorithms, future projects conducted through OCP's chip architecture project may eventually break the hold that NVIDIA GPUs and Google's TPU chips have on training large AI models.[62] As both companies' chips are manufactured at Taiwanese contract manufacturing fabs, with most production operated by TSMC, open chiplet architectures could feasibly allow for commoditized replacement from contract fabs in Taiwan and China.[63]

[60] Rogier Creemers, et al., Translation: 14th Five-Year Plan for National Informatization – Dec. 2021, DigiChina (2021).
[61] Accelerating Digitalization and Building a Digital China, China National Development and Reform Commission (2021).
[62] Jeffrey Burt, China Stretches Another AI Framework to Exascale, The Next Platform (2022).
[63] Jean-Luc Aufranc, UCIe (Universal Chiplet Interconnect Express) Open Standards for Chiplets with Heterogeneous Chips, CNX Software (2022).

Commoditizing the Entire Ecosystem Without an Industrial Strategy Will Further Erode U.S.-Based Manufacturing

Taiwanese and PRC manufacturers dominate commoditized hardware. Similar to open source software initiatives, OCP threatens to disrupt the business models of critical U.S. hardware companies, including Cisco, IBM, Dell, and HP, by handing Taiwanese and Chinese contract manufacturers (like Quanta, Inspur, and Foxconn) the core intellectual property they lack. Decades of competitive advantage and IP are under threat from OCP. Additionally, major PRC tech firms such as Baidu, Alibaba, and Tencent are now participating in OCP's server design and source-code development, further accelerating China's drive to dominate global computer hardware architectures. According to Microsoft, open server systems cost 40 percent less than traditional IT equipment.[64]

Software Paradigm Focused on Individual Malign Actors Insufficient for Addressing Nation-State Threats

Research in the field of hardware cybersecurity is currently focused on malign actors seeking to do harm, such as an insider attack led by one insider or a small group. The other predominant cybersecurity concern is an unintended flaw integrated into the chip's architecture during the design or fabrication phase that can later be exploited by outside actors. However, in the current contested global environment, an individual company-led response is not only inadequate, it is dangerous. In this regard, I further contend that **if a nation-state, whose industry dominates the production of major segments of the semiconductor fabrication supply chain, were to intentionally leverage this access to insert hardware trojans randomly across the entire ecosystem, it would be nearly impossible to mitigate.** At present, the U.S. Government has essentially outsourced our nation's cybersecurity implementation to the private sector. Sophisticated multi-vector errors are increasingly difficult to detect and mitigate using existing malicious code prevention schemas.

The PRC is currently the only nation-state with a global microelectronics manufacturing industrial base, technical sophistication, and ministries powerful enough to fully exploit this growing risk to global digital infrastructure. PRC officials are not subject to the same constraints and accountability mechanisms as their peers in rule-of-law societies, and law enforcement in China is subject to the Party's whims. Under Article 14 of the PRC National Intelligence Law (as amended in 2018), the Ministry of State Security (MSS) and other national intelligence institutions can request relevant organs, organizations, and citizens to provide necessary support, assistance, and cooperation.[65] Article 14 clearly states that it is illegal for PRC citizens or state-owned or private firms to refuse cooperation or deny the MSS access to facilities, digital networks, and related work products. Given the PRC's central position in the global electronics supply chain, the increasingly commoditized open source production ecosystem could grant the MSS – and by extension, the entire PRC government as a whole – the ability to access and potentially control much of the world's digital infrastructure. Given these real and growing vulnerabilities, we argue for a strategy that enacts deep technology restrictions to block the

[64] Microsoft's Open CloudServer, Microsoft at 5 (2015).
[65] People's Republic of China National Intelligence Law (as amended in 2018), China Law Translate (last accessed 2023); Nazak Nikakhtar, U.S. Businesses Must Navigate Significant Risk of Chinese Government Access to Their Data, Wiley (2021).

actions of a nation-state adversary. In other words, an approach that would wall out producers in countries of concern through market access restrictions in critical infrastructure is required.

The U.S. Lacks a Policy Approach to Open Source Hardware: Regulatory Oversight Is Needed

At present, the U.S. Government lacks both a policy approach to OSHW and an understanding of the vulnerabilities it poses. As a first step, the United States must act swiftly to undertake a national security review of OSHW initiatives, which are taking over U.S. and increasingly global digital infrastructure. The broader ecosystem of transformative technologies like IoT and 5G are fundamentally enabled by the backend digital infrastructure of routers and data processing servers, which are currently transitioning to open source-designed and produced hardware. Open source software and hardware have the potential to unleash great innovation and profit, but are predicated on open competition and do not account for national security.

To help secure U.S. leadership and safeguard the nation's core digital infrastructure from disruption, this rapidly evolving technology paradigm requires a new public-private framework that inculcates security requirements into the ecosystem without stifling innovation and healthy competition. Open source technology creates a "tragedy of the commons" wherein no one actor is responsible for addressing security vulnerabilities that open source designs present. When suppliers and technology partners cannot meet minimum standards of trust they should not be allowed to participate in the ecosystem. **To function properly, open source software – and to an even greater extent, hardware – rely upon the stored value provided by high-trust societies with strong independent regulatory frameworks, judiciaries, and the rule of law. When amalgamated with actors from low-trust societies lacking transparent regulatory frameworks and independent judiciaries, the disruptive nature of open source can easily be weaponized for malign ends.**

Policy Recommendations[66]

Organization: The U.S. Government should ensure it is adequately organized to mitigate the cybersecurity threat that OSHW produced in countries of concern may pose. Key steps for consideration:

- **The Department of Homeland Security (DHS) and Department of Defense (DOD) should undertake a national security review of OSHW initiatives and identify vulnerabilities related to critical infrastructure.** Congress and executive branch departments and agencies lack awareness of the threat OSHW may pose to U.S. critical infrastructure. A review should be led jointly by DOD and DHS. DOD should also prepare a report on mitigating risks OSHW may pose to U.S. military facilities and military operations.

[66] These recommendations are not intended to provide a comprehensive strategy to deal with the challenge, but are rather intended to promote further discussion and outline initial steps the United States should consider.

- **The U.S. Government should establish, and the Congress should provide funding for, a Center for Open Source Technology Security.** The Center would identify and catalog critical open-source software and hardware in need of support and fund improvements in cybersecurity.[67] Such an office could leverage a joint operations center model, bringing expertise to bear from across multiple relevant departments and agencies. While unable to respond to vulnerabilities at scale, a Center for Open Source Technology Security could focus on rapidly detecting vulnerabilities and notifying relevant actors.

Security Standards: U.S. authorities should set strong minimum rules and certification procedures for OSHW cybersecurity and verification. Key steps for consideration:

- **U.S. authorities should develop standards to ensure cybersecurity at the hardware level.** Policymakers should develop clear standards for open source hardware and identify or create bodies to certify OSHW devices – including the growing number of lightly regulated IoT devices – to avoid a race to the bottom of cheap, non-secure products. In 2022, a public-private partnership involving the National Institute of Standards and Technology (NIST) at the Department of Commerce and several U.S. technology companies completed a demonstration project for hardware-based cybersecurity and transparency using a 'Roots of Trust' approach.[68] This approach, which "securely bind[s] the device's attributes to the device's identity," is designed to allow the end-user to track the device's journey through the supply chain.[69] While not foolproof, this and other approaches can enhance supply chain traceability and increase the odds that vulnerabilities are detected. U.S. authorities should also work with allies and partners to align these standards and share best practices. NIST's ongoing work to update its Cybersecurity Framework, first released in 2014 and updated in 2018, offers a window to elevate and systematize efforts to address cybersecurity at the hardware level.[70] In addition, the U.S. Securities and Exchange Commission (SEC) should consider addressing OSHW risks in its requirements for companies to disclose cybersecurity incidents that have a material impact on their businesses to investors.[71]

- **Work with industry to set strong minimum security standards for ORAN hardware components and architecture.** Many U.S. policymakers, firms, and researchers see tremendous promise for Open RAN and open, programmable networks to bring more vendors into communications technology and reduce critical dependencies. Yet a network mixing hardware and software from multiple vendors potentially adds new complexity and risks to operators compared to proprietary, "vendor-locked" networks. This underscores the need for U.S. authorities to focus on security first in their promotion and

[67] Restoring the Sources of Techno-Economic Advantage, Special Competitive Studies Project at 39 (2022).
[68] Tyler Diamond, et al., NIST SPECIAL PUBLICATION 1800-34B: Validating the Integrity of Computing Devices, U.S. National Institute of Standards and Technology (2022).
[69] Tyler Diamond, et al., NIST SPECIAL PUBLICATION 1800-34B: Validating the Integrity of Computing Devices, U.S. National Institute of Standards and Technology (2022).
[70] Cybersecurity Framework, U.S. National Institute of Standards and Technology (last accessed 2023); Billy Mitchell, NIST Working on 'Potential Significant Updates' to Cybersecurity Framework, FedScoop (2023); Request for Information: Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management, U.S. National Institute of Standards and Technology (2022).
[71] Tom McKay, Forthcoming SEC Rules Will Trigger 'Tectonic Shift' in How Corporate Boards Treat Cybersecurity, IT Brew (2023).

testing of ORAN, setting high minimum standards for RAN components and networked devices in critical infrastructure.

Disclosure Requirements and Supply Chain Transparency: Require technology firms servicing critical infrastructure in the United States to disclose open source hardware used in their servers and networks, including detailed supply chain data, to increase transparency.

- **NIST should consider requiring federal contractors to increase supply chain transparency by disclosing a hardware bill of materials.**[72] In manufacturing, a "bill of materials" is a comprehensive list of inputs and components needed to build a product. A software bill of materials (SBOM) discloses all open source and third-party components present in a software application,[73] and the Biden Administration's 2021 E.O. on Improving the Nation's Cybersecurity recommended requiring federal contractors to disclose an SBOM.[74] A hardware bill of materials (HBOM) would include detailed information on security validations, design intent, and country of origin for a piece of hardware, granting increased visibility and enabling authorities to mitigate and more quickly address attacks.[75]

- **Strengthen Federal Acquisition Regulation (FAR) guidelines for reporting compromised parts to include commercial items, and extend the regulations beyond the Defense Department.** At present, reporting hardware-based electronics vulnerabilities is a voluntary exercise for federal contractors. The 2012 National Defense Authorization Act amended FAR to require contractors to report faulty or counterfeit parts to the Government-Industry Data Exchange Program (GIDEP), the official database used by DOD to report counterfeit electronics or other faulty components.[76] However, the final rule "does not require reporting of foreign corporations or entities that do not have an office, place of business, or paying agent in the United States,"[77] does not apply to commercially available items, and does not extend beyond the Department of Defense.[78] FAR guidelines should be expanded to fill these loopholes. Reform efforts could be led by the Federal Acquisition Security Council, an interagency body established in 2018 to develop policies for federal purchasing of information and communications technologies.[79]

---

[72] Initial Summary Analysis of Responses to the Request for Information (RFI) Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management, U.S. National Institute of Standards and Technology (2022).
[73] Fred Bals, What Is a Software Bill of Materials?, Synopsys (2022).
[74] E.O. 14028, Executive Order on Improving the Nation's Cybersecurity, The White House (2021).
[75] Andreas Kuehlmann, Hardware Bill of Materials: Essential in Electronics as Ingredients Are to Food, EETimes (2022).
[76] Pub. L. 112-81, National Defense Authorization Act for Fiscal Year 2012, § 818(c)(2); About GIDEP, Government – Industry Data Exchange Program (last accessed 2023).
[77] Susan Ebner, Final FAR Rule Mandating GIDEP Reporting of Actual or Suspected Counterfeit Parts Issued: More Questions Than Answers, JD Supra (2019).
[78] The FAR Council Adopts a New Rule on Reporting Counterfeit Parts or Critical Nonconforming Commons Items in the Supply Chain, Oles Morrison Rinker & Baker LLP (2020).
[79] Lee Sutherland, The Federal Acquisition Security Council: A Primer, Lawfare (2020).

Import Restrictions: Take steps to block OSHW components produced in countries of concern from being installed in U.S. critical infrastructure and systems used by federal contractors.

- **U.S. authorities should conduct an investigation into OSHW produced in countries of concern as a step toward blocking imports.**[80] Such an investigation could be conducted in one of two ways: first, the Department of Commerce has been delegated the authority, in conjunction with seven other departments and agencies, to block transactions that might impose "undue risks" of sabotage, subversion, or catastrophic effects on U.S. critical infrastructure, ICT providers, or the digital economy.[81] This would require a Department of Commerce information and communications technology and services (ICTS) investigation into OSHW produced in China. Second, under an FCC order, Team Telecom could initiate a review and add specific companies that pose an undue risk to U.S. networks to the Covered List.[82]

Domestic Investment: Increase investment in novel technologies and procedures designed to enhance hardware-based cybersecurity, supply chain traceability, and detection of vulnerabilities.

- **Increase R&D funding for hardware-based cybersecurity and traceability measures.** A number of U.S. Government projects designed to mitigate hardware-based cybersecurity risk already exist, but many remain in the research or pilot phase. DARPA's SSITH Program, for example – launched as part of the Electronics Resurgence Initiative – aims to develop a secure architecture for IoT immune to major hardware-based attacks, and has shown significant promise.[83] Likewise, the NIST hardware 'roots of trust' program, noted above, demonstrates that supply chain traceability at the hardware level is indeed possible.[84] Additional funding is needed to scale these and other initiatives and conduct further research on emerging approaches to hardware-based cybersecurity.

- **The Department of Commerce should identify secure microelectronics and hardware-based cybersecurity as a designated line of effort for the National Semiconductor Technology Center (NSTC).** Congress established the NSTC as a U.S. center of excellence to accelerate microelectronics prototyping and R&D.[85] Both the President's Council of Advisors on Science and Technology (PCAST) and the

[80] As a first step, the investigation should focus on OSHW produced in the PRC, where the Chinese Communist Party's (CCP) control over firms is most direct. However, such an investigation should also consider risks posed by chip fabrication (and related OSHW development) in third countries that may be subject to CCP control or malign influence, or unwittingly incorporate CCP-influenced logic design which may include a hardware trojan.
[81] E. O. 13873, Securing the Information and Communications Technology and Services Supply Chain, The White House (2019).
[82] E. O. 13913, Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, The White House, (2020); Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector - Frequently Asked Questions, U.S. Department of Justice (2021).
[83] Lok Yan, System Security Integration Through Hardware and Firmware (SSITH), DARPA (last accessed 2023); Samuel K. Moore, Darpa Hacks Its Secure Hardware, Fends Off Most Attacks, IEEE Spectrum (2021).
[84] Tyler Diamond, et al., NIST SPECIAL PUBLICATION 1800-34B: Validating the Integrity of Computing Devices, U.S. National Institute of Standards and Technology (2022).
[85] Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, § 9906 (2021); Pub. L. 117-167, CHIPS & Science Act of 2022, § 102 (2022).

Semiconductor Industry Association have highlighted secure microelectronics as a recommended research area for the Center.[86] "There is a tremendous opportunity for the design of secure semiconductor chips," notes PCAST. "To maximize effectiveness, security must be pursued as an integral part of design, not as an add-on after the chip is designed."[87]

[86] American Semiconductor Research: Leadership Through Innovation, Semiconductor Industry Association at 19-21 (2022); REPORT TO THE PRESIDENT: Revitalizing the U.S.Semiconductor Ecosystem, President's Council of Advisors on Science and Technology at 25 (2022).

[87] According to PCAST, a research agenda for secure microelectronics should include: "(1) design for fully secure end-to-end hardware and software solutions that are secure against various forms of attacks on operation, data, and communications; (2) security in the chip design tool chain that would enable end-to-end security solutions to be verified by design; (3) secure hardware supply chain covering chip fabrication, packaging, and system integration; (4) implementation of post-quantum cryptography; (5) implementation of low-power cryptography for secure communications and transactions; and (6) other privacy preserving hardware implementations for processing encrypted data." REPORT TO THE PRESIDENT: Revitalizing the U.S.Semiconductor Ecosystem, President's Council of Advisors on Science and Technology at 25 (2022).