25 YEARS | GCSP
Geneva Centre for Security Policy

Cyber Security Policy Brief

# The impact of regulatory frameworks on the global digital communications industry

Dr Robert Dewar and Ellie Templeton

WWW.GCSP.CH

# Contents

# Executive Summary

The imposition of commercial restrictions via national or regional regulatory frameworks has long been a tool of international diplomacy. National governments place commercial restrictions on the capacities of states and foreign-based corporate entities to engage in economic activities with the aim of compelling them to alter their courses of action. Due to their provision of critical national infrastructure such as digital networks, commercial technology companies can be of service to national security, but can also pose a risk. To better understand the impact of regulations and restrictions, this policy brief examines the restrictions imposed by three regulatory frameworks:

1. The package of measures instituted by the United States (US) from 2018, including the National Defence Authorisation Act, the Cyberspace Solarium Commission Report and the Clean Network Program;
2. The "Cyber Diplomacy Toolbox" and "Toolbox for 5G Security" initiated by the European Union under the aegis of its wider cyber security policy;
3. The operational restrictions placed on global digital technology platforms and regulatory security frameworks for network operators within China, including the Multi-Level Protection Scheme 2.0.

The restrictions explored in this policy brief have been imposed by these actors for different reasons. The US has applied access restrictions on private vendors deemed "high-risk" to remove or limit them from national digital networks and infrastructure. The EU has imposed economic sanctions in response to malicious cyber operations with the aim of both attributing and deterring such activity. China has imposed operational restrictions to protect digital sovereignty. It is also important to acknowledge that, at the time of writing, several of these measures – for example certain parts of the US Clean Network Program – are either newly deployed or not yet in place. As a result, data on these measures is limited and evaluation of their effects is problematic. Despite their varying objectives and recent release, these frameworks have had two significant common impacts.

The first is socio-political. Commercial restrictions are imposed within the context of geopolitical rivalries. As a result, they perpetuate a vicious cycle of mistrust between public and private international actors. Trust is lost between state actors, which leads to prioritisation of domestic vendors in local and international markets. This leads to restrictions being placed on foreign-based commercial entities, which leads to a further cooling of relations between state actors, leading to further commercial restrictions. This vicious cycle has reinforced deterrence-based policy approaches and normalised a presumption of untrustworthiness. The second impact is economic. Restrictions lead to delays in rolling out new innovations, such as 5G infrastructure, and hinders access to those digital innovations as well as increasing market insecurity as national and regional movements accelerate towards digital autarky.

These impacts also have consequences for cyber security. They hamper efforts to achieve consensus on effective international cyber security norms and protection standards, and risk the development of "splinternets" as digital security policies diverge and commercial access is limited. Such restrictions also weaken national cyber resilience and the resilience of the telecommunications and digital industries. This has wider implications for consumer and supply chain security, network resilience, digital fragmentation and technology standardisations.

Mitigating these impacts is a complex challenge, one which requires breaking the cycle of mistrust by accepting that restrictive tools intended to create secure environments may be counterproductive. It also requires the acknowledgement that, in the geopolitical climate of autumn 2020, systems of economic restrictions are blunt objects trying to hit moving targets. Whilst regulations for national critical infrastructures and industries will always be a necessity, regulatory frameworks more conducive to a globalised, innovative and highly agile industry and predicated on cyber diplomacy may better help nations and regions operate securely in the "fourth industrial revolution".[1]

# 1 Introduction

A range of regulatory frameworks have been imposed by national governments and intergovernmental actors to control the operations of the digital communications sector. Whilst exercising their rights to manage entities operating within their jurisdictions, the imposition of economic restrictions has a significant impact beyond limiting commercial operations.

This policy brief will analyse the impact of regulatory frameworks on the digital communications industry by exploring three high-profile programmes of restrictions imposed by three very different international actors:

1. The package of measures instituted by the United States (US) from 2018, including the National Defence Authorisation Act, the Cyberspace Solarium Commission Report and the Clean Network Program;
2. The "Cyber Diplomacy Toolbox" and "Toolbox for 5G Security" initiated by the European Union under the aegis of its wider cyber security policy;
3. The operational restrictions placed on global digital technology platforms and regulatory security frameworks for network operators within China, including the Multi-Level Protection Scheme 2.0.

It is important to acknowledge that, at the time of writing, several of these measures – for example certain parts of the US Clean Network Program – are either newly deployed or not yet in place. As a result, data on these measures is limited and evaluation of their effects is problematic. Nevertheless, it is possible to posit two important impacts for the digital industry and cyber security by examining the nature and targets of the restrictions.

The first impact is socio-political. **Trust, already limited between international entities in 2020, will be further diminished by a vicious cycle of rivalry and economic restrictions**. Due to the high number of malicious cyber operations currently being observed – and a widening of targets to include healthcare providers and health organisations[2] – trust and trustworthiness are at a premium. The Internet and the World Wide Web were created to share information, promote communication and enable a better understanding between communities, and so *enhance* trust. However, tools put in place to restrict access to commercial markets and measure entities' trustworthiness can be counter-productive because they reinforce deterrence-based approaches and **perpetuate a culture of mistrust**.

The second impact is economic; a consequence of **the politicisation of commerce**. By controlling the ability of specific entities to access certain markets as a result of geopolitical rivalries, **the pool of vendors able to provide the latest technology and services is reduced**. This risks inadvertently creating monopolies – something the EU seeks to prevent – as well as inhibiting the highest quality or most effective tools and components being used in national infrastructure. This in turn disadvantages civil society as the rollout and access to the latest advances – such as 5G – is impeded by restrictions placed on vendors at the forefront of technological innovation. Commercial restrictions also impact international trade, particularly as national and regional regulatory frameworks accelerate towards digital autarky.

**By controlling the ability of specific entities to access certain markets as a result of geopolitical rivalries, the pool of vendors able to provide the latest technology and services is reduced.**

These impacts also have consequences for global cyber security policy. Many aspects of human life are being lived through, and are dependent on, digital technology. Rather than bringing entities together to tackle the collective risk associated with this dependence, the **deployment of commercial restrictions is consolidating and normalising global divides and long-standing international rivalries**. An important part of the problem is that trust in global cyber security policy has been significantly eroded due to a number of high-profile cyber operations taking place between geopolitical rivals. In 2018, news reports emerged alleging that the CIA had been granted expansive powers to conduct cyber operations against China, Russia, Iran and North Korea.[3] On the other side of this traditional rivalry, two Chinese nationals were indicted for a series of hacking activities including targeting American defence contractors, allegedly with the support of Chinese authorities.[4] The imposition of economic restrictions or sanctions as responses to these operations can exacerbate an already fractious policy agenda. This compromises the ability to build a framework for cooperation, achieve network resilience or rebuild trust between international entities, thereby further reducing the chances of achieving consensus on global norms.

The lack of agreement on international cyber security norms and frameworks **risks creating a "splinternet"**,[5] a series of separate national or regional networks subject to different legal, social and normative regulations. Were this to occur, it would amplify the challenges already faced when seeking international consensus on industrial cyber security norms and corporate behaviour as well as cyber security standardisations in new technological innovations. This has long-term consequences for the **resilience of the globalised and interconnected communications networks**. Whilst commercial restrictions aim to enhance national and regional resilience, they also increase the potential for new systemic risks to digital security.

2

# What are economic restrictions and why use them?

The purpose of economic restrictions or sanctions is to alter the commercial relationship between states[6] by preventing the sanctioned state or state-based entity from engaging in specific commercial activities. The intention is to deter the actor from a particular course of action or compel a change in policy or behaviour. Regulatory restrictions, including economic sanctions, are also imposed against those deemed to be in breach of international law, and are designed to compel that actor – usually a state – to return to conformity.[7]

The use of commercial restrictions as a tool for diplomacy or foreign policy is nothing new. From the 1850s the term *blockade* was used to describe measures used to interrupt normal commercial activity between entities "legally on peaceful terms",[8] i.e. not in a state of war or conflict. Two often cited 20th century examples of economic restrictions imposed to effect geopolitical change are the 1973 oil embargo instituted by OPEC countries and the global embargoes placed on South Africa by the United Nations (UN) in 1987.

In recent decades, however, commercial restrictions have been imposed to regulate *private* actors, particularly those that provide elements of critical state infrastructure and services. Due to industrial and digital globalisation, technology companies have become global conglomerates with financial resources and digital capacities that rival – and even exceed – those of nation states.[9] Corporations are engaging in geopolitical discussions at an unprecedented level.[10] There is concern that commercialised digital technology and innovation is being concentrated in too few mega-corporations,[11] reducing investment choice and concentrating the control and development of global communications infrastructure and networks in a few specific entities. States seek to exercise an element of control over these corporations and their commercial activities by putting in places programmes of commercial restrictions and regulations.

However, regulations to control and restrict commercial operations have impacts beyond the immediate restriction of an entity's room for commercial manoeuvre.[12] To analyse this wider impact, this policy brief will focus on three systems of commercial restrictions.

## 2.1. Current Regulatory Frameworks: The United States

The US has recently expanded national regulatory frameworks, in both the range of available tools and their international scope. One prominent tool is the **National Defence Authorisation Act (NDAA)**, an annual series of US federal laws detailing the Department of Defense's annual budget and expenditures. The NDAA for Fiscal Year 2019 was signed into law on 13 August 2018.

As part of the NDAA for Fiscal Year 2019 the **Cyberspace Solarium Commission (CSC)** was appointed to "develop a consensus on a strategic approach to defending the United States in cyberspace".[13] The Commission published its strategic report on 11 March 2020, reinforcing the 2018 Department of Defence Cyber Strategy to "defend forward".[14] This is to be achieved through a layered cyber deterrence approach; shaping the digital environment, denying benefits and imposing costs.[15] The Commission report outlines 82 policy and legislative recommendations across six strategic pillars, which seek to reform the US Government's approach to cyber security following Congressional enactment.[16]

**The NDAA is part of a range of protectionist tools regulating digital firms operating in the mainland United States.**

The NDAA for Fiscal Year 2019 also signed into law **Section 889**, which aims to shield national telecommunications and surveillance systems from the risks posed by specific non-US technological and industrial entities. It introduced a prohibition on the federal government, its contractors and grant or loan beneficiaries from procuring or using "telecommunication equipment or services as a substantial or essential component of any system, or as critical technology as part of any system"[17] that are produced or provided by five specific telecommunications companies and their subsidiaries. These five companies are Huawei, ZTE, Hytera, Hikvision, and Dahua.

This prohibition has been implemented in two phases. On 13 August 2019, Section 889(a)(1)(A) came into force. This enforced the ban on federal government's direct procurement or use of these five companies. The second phase under Section 889(a)(1)(B) became effective exactly a year later on 13 August 2020 and extends the governmental prohibition to contracting with any entity that themselves procure or use these equipment or services to the relevant thresholds.[18]

The NDAA is part of a range of protectionist tools regulating digital firms operating in the mainland United States. In 2019, the Bureau of Industry and Security established an 'Entity List' limiting exports of US-manufactured products to specific non-US telecommunications entities and associated affiliates, unless a temporary licence is obtained. The Department of Commerce also imposed industrial sanctions through the amendment of the **Foreign-Produced Direct Product Rule (FDPRA)** in May 2020. This Rule prohibits all US firms or any global manufacturer using American-built chipmaking equipment from trading "direct products of controlled US technology or software" with Chinese-based telecommunications firm Huawei and its relevant subsidiaries.[19]

The most recent tool implemented by the US is the **Clean Network Program (CNP)**. Unveiled on 5 August 2020, the Program contains a five-pronged approach to protect US critical information and communication technology and seeks to reduce exposure from perceived "malign actors".[20] These measures include:

1. Clean Carrier (ensuring certain carriers are not connected to US telecom networks);
2. Clean Store (removing "untrusted" apps from US app stores);
3. Clean Apps (stopping "untrusted" smartphone manufacturers from pre-installing or making US apps available);
4. Clean Cloud (preventing information being stored on cloud-based services that are accessible to foreign adversaries);
5. Clean Cable (ensuring undersea cables are not subverted for intelligence gathering).[21]

**The collection of EU's regulatory frameworks aims to ensure that Europe, and the industries and consumers within it, are "fit for the digital age".**

By autumn 2020, the US confirmed that over 30 countries and territories had joined the Program as "Clean Countries".[22] These nations commit to the use of specified "Clean Telco" vendors in their prospective 5G networks and digital infrastructure.[23] The Program aims to be the new strategic framework for wider national regulatory tools, particularly for the enforcement of economic restrictions on specific non-US commercial entities, limiting access to internal markets and national telecommunications systems and infrastructure.

## 2.2. Current Regulatory Frameworks: The European Union

The European Union (EU) employs a number of regulatory frameworks governing the digital communications industry in relation to cyber and digital security. The most prominent are the **General Data Protection Regulation (GDPR)** and the **Directive on Security of Network and Information Systems (NIS Directive)**.

The GDPR came into force in May 2018 and specifies the necessary personal data and privacy protection requirements for commercial entities operating within Europe. The NIS Directive is a companion document to the EU's Cyber Security Strategy of 2013, addressing the security of systems. The Directive was enforced in August 2016 and ratified by Member States in May 2018. It established a systems and cyber security regulatory framework for the operators of essential services and other digital service providers.[24] The GDPR and NIS Directive are legislative instruments that apply to commercial entities both operating within, or providing goods or services to, any Member State. They therefore act as commercial regulations affecting a significant proportion of the transnational entities within the telecommunications and digital market.

In addition to these legislative regulations, the EU is increasingly employing a hardened stance in relation to cyber security. As an economic entity, the EU relies on fiscal measures to respond to malicious cyber activities. In June 2017, the Union introduced the **Cyber Diplomacy Toolbox (CDT)** as a joint diplomatic action to address these activities. The Toolbox contains a range of instruments, including sanctions mechanisms such as travel restrictions and asset freezing. Its central purpose is to enhance both "signalling and reactive capacities" to influence the behaviour of potential aggressors *and* collectively respond to malicious cyber incidents.[25] In July 2020, the European Council used the provisions of the Toolbox for the first time to impose economic sanctions on six individuals and three entities from Russia, China and North Korea for alleged involvement in cyber operations targeting EU entities.[26]

In addition to the CDT, the European Commission established the **EU Toolbox for 5G Security** in January 2020. This Toolbox details a mitigation plan and provides both strategic and technical measures to be adopted by Member States when rolling out 5G technology based on a coordinated risk assessment of infrastructure and systems. It is predicated upon ensuring that Member States can "restrict, prohibit and/or impose specific requirements and conditions, in accordance with a risk-based approach".[27] Actions include the strengthening of national security requirements and vendor diversity, but paradoxically includes measures to restrict suppliers considered to be "high risk" and manage their involvement in assets defined as "critical and sensitive".[28] The collection of EU's regulatory frameworks aims to ensure that Europe, and the industries and consumers within it, are "fit for the digital age".[29]

## 2.3. Current Regulatory Frameworks: The People's Republic of China

To promote compliance, China has been a strong advocate for self-regulation within the digital industry.

China's regulatory frameworks have employed a "state-centric strategy for comprehensive informationisation", which has ensured state oversight of Internet usage and digital infrastructure.[30] The concept of "internet sovereignty" has been an important factor in this strategy.[31] Based on legislative frameworks from 1996, digital regulation has developed in accordance with the expansion of the Internet.[32] As such, a number of measures control the access to Chinese digital space of identified foreign corporations. This has included restricting or regulating worldwide platforms such as Facebook, YouTube, Google and BBC News.[33] Other corporations and domains have been both granted and denied access over time, based on compliance with the necessary national regulations. To promote compliance, China has been a strong advocate for self-regulation within the digital industry. Several self-regulatory measures have been released including the **Public Pledge on Self-Regulation and Professional Ethics for China Internet Industry**.[34] This places responsibility on digital companies to self-regulate in order to abide by national requirements.

Further regulatory frameworks have been enacted to better protect national networks, safeguard commercial and consumer rights and enhance cyber security. New operator security requirements were adopted in the **Cyber Security Law of the People's Republic of China**.[35] In December 2019, the **Multi-Level Protection Scheme (MLPS) 2.0** was introduced. It aims to address the associated security risks of newly developed technologies, including "networks, information systems, cloud platforms, the internet of things, control systems, big data and mobile internet".[36] The MLPS updates China's regulatory risk-based approach to the industry, including in the security classification of networks and the monitoring of commercial operators.[37] The objective of these measures, including economic restrictions, is to protect Chinese sovereignty over its national information networks and to ensure that only trustworthy vendors and entities are able to operate in China's digital space.

The frameworks imposed by these three regulatory actors show the diverse objectives and application of commercial restrictions on industrial entities. Whilst the *types* of tools – economic sanctions, lists of proscribed entities – are not new, several of these programmes were just entering into force at the time of writing. This can make the assessment of impact problematic. Nevertheless, based on an examination of the regulatory objectives and target entities, it is possible to posit important impact trends and what these could mean for cyber security moving forward.

# 3 Impacts of regulatory frameworks

As companies operating in a globalised market, today's telecommunications providers are subject to the legislative and regulatory frameworks of the regions in which they conduct business. Whilst this is true of any commercial sector, the critical nature of telecommunications and digital infrastructure to the resilience and basic functioning of a state has attracted increased scrutiny. Compared to industries such as automobile or clothing manufacturing, which enjoy relative freedom of operation, the impact of regulatory frameworks on private telecommunications companies is both amplified and idiosyncratic. There are two primary impacts on the industry; socio-political and economic.

## 3.1. Socio-political impacts

Recent regulatory frameworks have demonstrated a dichotomous situation for technology companies. Due to their provision of critical national infrastructure such as digital networks, these providers are a *service* to national security, but can also pose a *risk*. Digital innovations are considered as commercially "strategic assets".[38] However, as state functionality becomes increasingly dependent on the equipment and systems produced by private technology companies, they also pose a new type of risk if exploited. As a result, the first casualty of commercial restrictions targeting commercial entities in a sector vital to national resilience and security is the loss of **trust**.

### 3.1.1. Continuing the vicious cycle of mistrust

Systems of economic restrictions or sanctions signal that the targeted commercial or state entity is a risk due to concerns about their practices. This demonstrates a loss of trust on the part of the regulator. If there are concerns about the level of foreign state control over an ostensibly commercial entity, that entity can be considered untrustworthy, and its access to markets limited. However, regulatory frameworks and sanctions that restrict these commercial activities are not imposed in a vacuum.

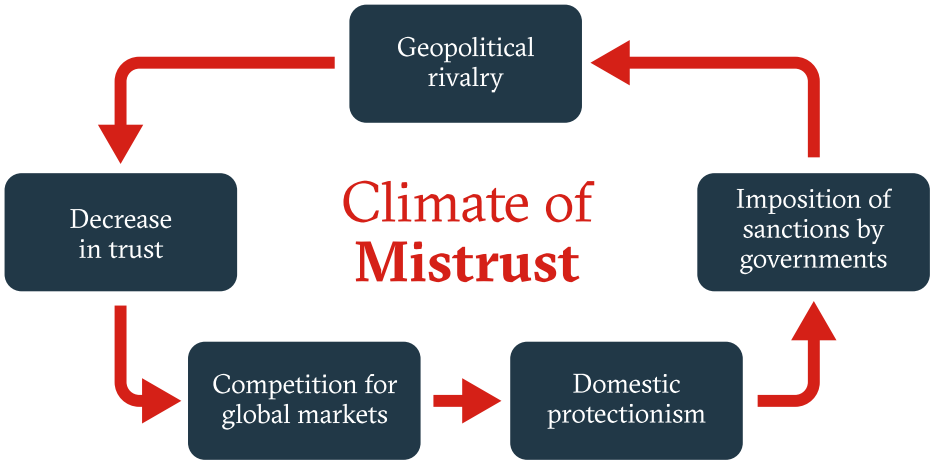
Restrictions targeting specific corporations are frequently used in response to a particular event or series of events that reduced trust in either the company itself or its country of origin. Often, this is the result of a wider geostrategic rivalry. This can be seen in the responses to allegations of IP theft by Chinese entities[39] or the apparent weaponization by the US of

Chinese dependence on its technology markets.[40] The resulting regulations affecting these two global powers are unilateral tit-for-tat actions which exacerbate an already low level of trust between them. Unless efforts are made to break this cycle, the tendency towards mistrust appears destined to continue, particularly in the field of digital innovation.

With 5G connectivity predicted to become the "backbone of our modern life and global trade", unprecedented attention has been drawn to the digital marketplace and its political value and influence.[41] It has emerged as a sector replete with geopolitical proxies. South Korea halted the import of key technologies from Japan in 2019 in response to its delisting as a "trusted trade partner".[42] India banned 118 Chinese mobile apps, based on perceived cyber security threats in the immediate aftermath of military border clashes between the two regional powers in the Himalayas in June 2020.[43] China's current exponential rise in technological innovation can be interpreted as moves to attain or retain a Great Power status[44] and increase its geopolitical influence in arenas such as the UN.[45] Likewise, US market restrictions target entities from its long-standing political and economic rivals, including China, Russia, Iran and North Korea.[46]

**The challenge for policymakers and commercial entities is that, if these regulatory arrangements are imposed as a result of geopolitical rivalries, the climate of mistrust is perpetuated in the regulatory frameworks themselves.**

The challenge for policymakers and commercial entities is that, if these regulatory arrangements are imposed as a result of geopolitical rivalries, the climate of mistrust is perpetuated in the regulatory frameworks themselves. The restrictions feed this presumption of untrustworthiness and create a functional spill-over, manifested by a vicious cycle of distrust. A specific incident such as a malicious cyber operation targeting state infrastructure starts a geopolitical chain-reaction leading to a cooling of relations between states. This leads to a geopolitical rivalry characterised by a decrease in trust and diplomatic activity. This global rivalry leads to competition, for example, in access to international markets or between vendors of similar services. This is manifested in the reluctance to provide access to internal markets to companies from the rival state. Therefore, sanctions are put in place to formalise this restriction. Such sanctions are imposed by government entities, which leads to a further breakdown in relations – and trust – between the states.




By this point in the cycle, re-establishing trust is a much greater challenge. In the case of digital commerce, the loss of trust is currently becoming normalised, with state and economic entities operating under a presumption of untrustworthiness, a presumption not helped by the empirical reality that malicious cyber activities are still occurring.[47]

### 3.1.2. The "presumption of untrustworthiness" leads to a new form of deterrence

A climate of digital mistrust coupled with an exponential rise in malicious cyber incidents has also revived a deterrence-based approach to regulating the digital space. This effect has been observed in all three regions explored in this policy brief. The Cyberspace Solarium Commission's three-layered cyber deterrence approach is designed to shape behaviour, deny benefits and impose costs.[48] Unlike prior CSC reports endorsing a single approach, the 2018 Commission adopted an "all-of-the-above" methodology, aiming to widen the national toolbox to include market forces, regulation, punitive measures for those who violate established cyber norms.[49] Similarly, China's Ministry of Commerce has warned of import controls being placed on the equipment of two leading European telecommunication companies, Nokia and Ericsson, if the EU were to restrict Chinese-based vendors from its digital market.[50] Finally, both the EU's Cyber Diplomacy and 5G Toolboxes seek to deter "the behaviour of potential aggressors" and mitigate risk in the development of 5G infrastructure.[51] Despite positive aims to protect specific markets, these "defend forward" approaches[52] further reinforce a presumption of untrustworthiness in the actors involved in the globalised communications and digital sector.

**A climate of digital mistrust coupled with an exponential rise in malicious cyber incidents has also revived a deterrence-based approach to regulating the digital space.**

Yet, such restrictions extend beyond hardware provision. China's longstanding separation of its "domestic cyberspace" from the "foreign cyberspace" is based on the concern that certain entities or individuals will use the Internet and the WWW to publish "harmful information" and disseminate "harmful activities" online.[53] Notably, the Self-Regulation Pledge can be considered a deterrent-based enforcement technique, compelling companies to impose restrictions on their own activities in order to avoid both economic and legal consequences, with one of the four "principles of self-discipline for the Internet industry" being a capacity to demonstrate "trustworthiness".[54]

This pervading culture of assuming the worst is already reaching its nadir. In 2019, the government of the Czech Republic published a series of proposals following its 5G Security Conference in Prague.[55] This was followed in May 2020 by the US Center for Strategic and International Studies (CSIS) publishing a "Criteria for Security and Trust in Telecommunications Networks and Services".[56] Both documents have positive and laudable goals. The Prague Proposals seek to create a safe and secure digital environment for 5G technology to be effectively and properly deployed, and the CSIS Criteria aims to provide policy and lawmakers with an effective metric for judging the trustworthiness of technology vendors.

National attempts to measure "trustworthiness" are also reflected in the implementation of China's MLPS 2.0. Network operators are required to classify the security of their networks in order to better assess and manage risk. However, under the new framework, what constitutes as "critical" has been widened and the threshold for operators requiring governmental monitoring has been lowered.[57] In a move similar to the trustworthiness metric advocated by the CSIS criteria, if operators do not meet regulatory requirements, they are added to a published list of "poorly performed" and "dishonest" – i.e. untrustworthy – companies.[58] As of April 2020, a number of central provisions were still in draft form,[59] making identifying concrete examples difficult.

The CSIS Criteria and the Chinese MLPS 2.0 therefore have wider implications for the global digital industry. Creating a list of 31 measurements of trustworthiness[60] – as the CSIS Criteria does – implies

that vendors' access to markets is based on a trustworthiness "score", a sliding scale in which one can lose 'trust points' if not all criteria are met. This system could place commercial entities at risk of losing lucrative contracts to other vendors with a higher 'trust score'. As a result, criteria for measuring trust may eventually be found to be counterproductive as they perpetuate a presumption of untrustworthiness and a system of evaluating industrial standards on confidence rather than quality. It is yet to be seen whether this approach to regulating commercial entities is able to stabilise an operational level of trust, and in turn, build confidence in the globalised digital communications industry.

## 3.2. Economic impacts

Operating in an environment where the prevailing narrative is negative and filled with statements pertaining to untrustworthiness has two kinds of economic impact; impeding commercial and social access to the latest digital innovations, and accelerating national and regional movements towards digital autarky and its subsequent effect on international trade practice and security.

**Security concerns raised as part of the culture of mistrust have resulted in the inconsistent exclusion of leading industrial vendors and equipment manufacturers from different nations.**

### 3.2.1. National economic and social impacts

Security concerns raised as part of the culture of mistrust have resulted in the inconsistent exclusion of leading industrial vendors and equipment manufacturers from different nations. Whilst investment in alternative, domestic digital providers can build national internal confidence, narrowing the market can have wider national economic implications, such as operational delays, rising costs for digital services and restricting competition. This was a particular concern following the UK's recent decision in July 2020 to remove hardware components from current 5G infrastructures produced by one specific vendor, Huawei.[61] As a result, 5G rollout is expected to be delayed by two to three years from 2020, with an additional expenditure of up to £2 billion required to remove the proscribed technology by 2027 from national networks.[62]

If this policy is repeated elsewhere, there may be consequences not only for the national installation of the latest digital communications, but also an inevitable impact on infrastructure providers who have tailored their products and expertise to strengthen particular commercial and social markets. Highly digitalised economies such as the EU, the US and China rely on the latest technological innovation being available. However, disincentivising innovators and causing delays in national digital developments risks leaving nations or regions behind the curve of global telecommunications advances. This can reduce the attractiveness of these markets both to consumers as users of the technology and to potential investors. Commercial entities may instead seek to insulate themselves from specific regulatory jurisdictions and tailor their end-products to alternative markets.

A further side-effect of the commercial isolation of untrusted vendors is that targeted entities may look not only to new markets for their products, but to new research and development (R&D) partners and beneficiaries. Global reconfigurations in response to recent sanctions are already becoming apparent, with personnel and investment being reassigned to more permissive regions and R&D platforms.[63] One example is increased Sino-Russian industrial cooperation.[64] Such commercial shifts can have wider long-term ripple effects on local employment, the regional exclusivity of digital R&D, as well as on global trade dynamics.

### 3.2.2. International trade impacts – a move to autarky

According to a recent press release, the May 2020 US FDPRA restrictions were formulated to strategically target the globalised, yet niche, semiconductor industry.[65] The sanctions prevent both domestic and international firms with American-built equipment from trading with Huawei and its subsidiaries. As a private entity heavily reliant upon the US production of semiconductor chips, the regulation is intended to affect the corporation's manufacturing of distributed end-products and subsequent trading capacities. However, commercial restrictions that target niche sectors – such as a single, narrow part of a globalised supply chain – can generate far-reaching disruptions to international trade, with for example, US firms set to lose US$ 7 billion in contracts.[66]

**The upshot of this situation is that the imposition of commercial restrictions, whether they incentivise local firms or discourage foreign investment, generates market uncertainty.**

The sanctioning of specific vendors also risks unintended consequences at the state-level. Tit-for-tat trade retaliation is already being observed following accounts that China is preparing to place US companies – including Apple, Qualcomm and Cisco – on its "unreliable entity list". This would impose corporate restrictions on industrial production and trade within China, as well as enforce compliance with Chinese cyber security and anti-monopoly laws.[67]

The regulation would affect digital commerce in two ways. First, it could force changes in the manufacturing and operational goals of listed vendors. Second, it may accelerate nation states' drives for domestic vendor reliance. The second effect is being seen in China, where the government is reported to be working towards national self-sufficiency in semiconductor production as part of its resolve to establish "an independent technology ecosystem".[68] The Chinese government recently pledged to invest over a trillion dollars in the industry and revise export restrictions.[69] The US has similarly demonstrated an increased push for digital autarky with the restriction of movement on US technology and trade through its range of regulatory tools. Following the NDAA and Clean Network Program initiatives, the US is also seeking to establish a domestic 5G vendor capable of providing the technology equipment needed. Potential providers include the European vendors Nokia and Ericsson, which already have a US presence.[70] This provides an important counter-argument to the criticisms levelled against those states or regions which do not permit market access to "foreign" manufacturers: local companies may be *incentivised* to invest in developing new technologies and produce hardware and software to replace that required to be removed.

The upshot of this situation is that the imposition of commercial restrictions, whether they incentivise local firms or discourage foreign investment, generates market uncertainty. This is not conducive to an attractive digital economy. The new restrictions and regulations about to come into force risk stimulating moves towards stockpiling, examples of which have already been seen as a reaction to uncertain commercial futures.[71] With the NDAA also authorising the extension of sanctions to further commercial entities "when applicable", in a similar manner to the EU's Toolbox sanctions, and China regulating access to its digital space, the telecommunications and digital industry will be characterised by economic insecurity as states vacillate between international trade frameworks and policies promoting digital autarky.

# 4 What does this mean for the future of cyber security?

## 4.1. Cyber security policy: creating a "splinternet"

As economic entities are dependent upon the jurisdictions in which they operate, it is important to consider the impact of commercial restrictions on cyber security policy. The US, China and EU recognise the importance of cyber security and data. The US CSC Report aims to avoid a "cyber 9/11" situation,[72] China's MLPS updates national data security practice and the EU NIS Directive and subsequent toolboxes aim to bolster "cyber security and resilience of 5G networks".[73] Many tools designed to maximise resilience are based on a consensus of internationally agreed norms and practice for the global digital industry.[74]

The development and imposition of commercial restrictions idiosyncratic to specific geopolitical regions can, however, reinforce disparities between already varying digital security practices, rules and standards. One example is the existing differences between data privacy frameworks such as the U.S. Clarifying Overseas Use of Data (CLOUD) Act and the EU's GDPR. Introduced two months prior to the GDPR, the CLOUD Act can compel service providers to disclose data stored on servers outside of the U.S. This contravenes GDPR regulations in the protection of individual's data and its transfer to third countries.[75] Such discrepancies were highlighted in the European Court of Justice decision in July 2020 to override the "Privacy Shield" – a data transfer regime between the EU and US – based on the inadequacy of personal data protection provided by US law.[76]

Such policies jeopardise the future of international standards in cyber security and technological innovations. Standardisation bodies such as the 3rd Generation Partnership Project (3GPP), and the European Telecommunications Standards Institute (ETSI) – which specify industry security standards for mobile communications and 5G developments – are caught in the crossfire in debates between partners from Europe, the US, China, Japan, South Korea and India. Complications arise when sanctioned private actors hold the majority of global 5G patents and lead the way in specific technological advancements. Recent US policy amendments allow American companies to cooperate with nationally restricted vendors in setting 5G standards.[77] However, if current sanctions frameworks derail international trade practices, it is conceivable that regional or even national standardisations will start to emerge. On a digital level, this could lead to what communications technology observers have labelled a "splinternet": the breaking up of the Internet and World Wide

Web into areas of different governance systems and networks along an "east-west split in the architecture of the Internet".[78]

A recent Chinese initiative may fuel this fragmentation, despite aims to the contrary. On the 8 September 2020, Chinese State Councillor and Foreign Minister Wang Yi announced in an international seminar on "Seizing digital opportunities for cooperation and development" a "Global Initiative on Data Security".[79] Aiming to address new challenges posed by increasing digitalisation, the initiative seeks to ensure data security and promote the digital economy. The Chinese Foreign Ministry spokesperson Zhao Lijian added that the "initiative aims to safeguard global data and supply chain security... and provide a blueprint for the formulation of global rules".[80]

The initiative is intended to demonstrate China's commitment to safeguarding global data security, and it calls upon other nations and the industry to support it and share responsibility for security through "bilateral, regional and international agreements".[81] Whilst a succinct and very new published initiative (at the time of writing) it provides eight core suggestions for states and ICT providers to adopt, tackling the issues of data security, corporate and state responsibility and patterns of good online behaviour.

The new initiative is, however, another set of norms being proposed and promoted in an increasingly crowded field. The Global Commission on the Stability of Cyberspace[82] and the Digital Geneva Convention[83] have advocated similar norms of state and corporate online behaviour. A problem is that many of these initiatives overlap, adding confusion to moves to achieve consensus which, coupled with the various different metrics of trustworthiness (such as the CSIS Criteria and MLPS 2.0) can have direct tangible effects on core cyber security goals, such as network resilience.

The imposition of restrictions or sanctions requires commercial entities to continuously reformulate their products and services to accommodate new regulatory frameworks.

## 4.2. Cyber resilience: creating contemporary risks

The imposition of restrictions or sanctions requires commercial entities to continuously reformulate their products and services to accommodate new regulatory frameworks. This uncertainty has implications for national cyber resilience capabilities. In January 2020, the UK endorsed a risk-balanced strategy for national 5G network and infrastructure development, based on cyber-expert intelligence and assessments conducted by the National Cyber Security Centre (NCSC). With the Centre co-ordinating an established monitoring system for national telecommunications vendors, the strategy maintained a balance between the best-suited, specialised equipment and the security risk posed by non-UK manufacturers. A decision was made to restrict the extent to which equipment from "high-risk" vendors could be installed in UK networks critical to national security, and to cap single-vendor inputs at 35% to maintain "resilience through supplier diversity".[84] The Government's replacement decision in July to remove all equipment from "high-risk" vendors from national networks, however, was premised on the impact of the FDPRA on the NCSC's initial mitigation strategy and subsequent ability to measure risk as the industry reshapes.[85]

While this may be logical from a cyber security resilience perspective, one of the criticisms levelled at the UK Government is that the replacement of key components already installed in UK digital infrastructure risks deploying equipment from alternative, insecure sources in a limited 5G-capable vendor market.[86] Blanket restrictions such as bans on certain suppliers or manufacturers may not take into account the specialised and risk-assessed nature of the components these companies produce; different manufacturers do not produce like-for-like hardware. The risk to digital resilience has been identified by a leaked national intelligence services report advising that a rushed replacement of 5G equipment

could result in the installation of more "untrusted technology that could increase the risk to the UK",[87] compromising its digital resilience. As Dave Aitel, an offensive cyber security expert cautioned, "you have to get your supply chain security *exactly* correct".[88]

National regulation designed to protect critical digital infrastructure is hamstrung by the globalisation of supply chains in the digital industry. Software and hardware development are routinely outsourced and specific nations have become well-known specialists in distinct component production and assembly processes. To remove specific entities from global supply chains requires not only state-level trust in the private sector, but transnational regulation and enforcement. Unless well executed, both industrial transparency[89] and unfamiliar substituted technologies along digital supply-chains could create systemic risks for digital security.

**National regulation designed to protect critical digital infrastructure is hamstrung by the globalisation of supply chains in the digital industry.**

5

# Conclusion

Regulatory frameworks and economic restrictions occupy a complex space in international relations. On one hand, they are measures designed to protect and secure elements of a nation's critical infrastructure, such as digital communications. On the other, they are punitive measures, designed to compel an actor to behave in a certain way or prevent a particular course of action. The socio-political and economic impacts of these frameworks, as well as their effects on cyber security, need to be better understood.

Ensuring safe, secure and viable digital communications networks is essential for international commerce, intergovernmental cooperation and daily life in the 21st century. At the time of writing, state responses to the COVID-19 pandemic further highlight the importance of effective and resilient telecommunications networks and digital services, and demonstrated the need to promote digital capacities in recovery roadmaps across the world.[90]

Commercial vendors are therefore being given increasing levels of responsibility to provide infrastructure and services vital to the normal functioning of a state or, in the case of the EU, entire regions. This is a particular issue for the rollout of 5G. States and regional entities exercise and protect their sovereignty by retaining the right to select and regulate which vendors provide core services, components or equipment to facilitate that connectivity.

Nevertheless, the metrics by which entities are being judged "trustworthy" and the deployment of deterrence-based economic tools are having wide -scale effects beyond the initial restriction of commercial movements. Socio-political and economic impacts such as rising costs and delays to the roll-out of new technologies, or the fragmentation of global digital markets and economic partnerships, are the consequences of regulatory frameworks predicated upon mistrust. These impacts will continue to affect cyber security as digital industry adapts and as states and international actors move towards new forms of digital autarky. This will hamper the resilience of national infrastructure, networks and digital services and could generate a new wave of contemporary digital risks.

Despite having a long history of use, there is an ongoing debate as to the effectiveness of deploying economic restrictions to further foreign policy and security objectives. Evenett makes the point that the level of influence on the policymakers of the sanctions' targets is still a matter of debate.[91] If this is the case, the usefulness of sanctions as tools for international foreign policy is called into question. Nevertheless, such tools continue to be used irrespective of their success in effecting geopolitical change. What is certain is that these economic restrictions are having real consequences and impact beyond their immediate remit. There are, however, two possible ways to move forward.

## 5.1. Break the cycle and re-establish trust

The current system of regulations and economic restrictions brings into focus the need to break the vicious cycle and re-establish trust among international actors. Whilst there are diverse regulatory approaches in the digital industry, as exhibited by the three frameworks examined in this policy brief, the vicious cycle of geopolitical rivalry and imposition of economic restrictions must be addressed. Whilst there are many reasons to do so, including mitigation of the subsequent socio-political and commercial impacts, one communal incentive is consumer trust. For civil society, online trust is a worldwide affair.

Whilst there are diverse regulatory approaches in the digital industry, as exhibited by the three frameworks examined in this policy brief, the vicious cycle of geopolitical rivalry and imposition of economic restrictions must be addressed.

With autarky being incompatible with today's globalised economic structure, international actors will be better served by cyber diplomacy to establish a level of trust acceptable to most, if not all, national policy requirements such as free market access and maintaining national digital sovereignty. Programmes of wide, indiscriminate restrictions are not conducive to this goal, and can be counterproductive.

Moreover, as the "fourth industrial revolution"[92] of innovation and transnational interconnectivity continues and gathers pace, strengthening global collaboration and governance systems to address systemic security risks and standardisations of new technology will be indispensable for cyber security. Such unity will in turn promote partnership confidence, protect innovation, safeguard consumers, and increase global resilience. Moving forward, the new normal should be based on achieving the best means for this operational level of collective digital trust.

## 5.2. Acknowledge that current systems of commercial restrictions are blunt objects trying to hit a moving target

As of autumn 2020, it is important to recognise that a number of the regulatory frameworks addressed in this policy brief are new, or still being introduced, to the digital communications field. Several of the CSC cyber security proposals are, at the time of writing, still in discussion in both houses of the US Congress, with the majority of actionable measures yet to be determined.[93] The European 5G Toolbox was adopted in January 2020 with Member State progress reviews currently underway;[94] the US Clean Network Program was announced on the 5 August and Section(B) of the NDAA instituted on the 13 August; and China proposed the "Global Initiative on Data Security" on the 8 September.[95] The programmes themselves are subject to change with shifts in national and regional priorities, particularly as the COVID-19 pandemic continues to transform global policy agendas.

The extent of the impact of these policies, inherently transnational in scope and initiated amidst a global pandemic, is yet to be seen. As industrial reactions begin to take shape, enforcement will require widescale monitoring, assessment and regulation as vendors reform, new industrial leaders emerge, and consumer demand shifts. Monitoring

the entities developing critical infrastructure will always be a security necessity. However, using economic restrictions as regulatory tools has the tendency to be either so specific in nature that they require complex workarounds, or so general that they cause more problems than they solve. When applied to a sector predicated upon high-speed innovation and technological globalisation, economic restrictions and sanctions will be consistently behind the curve. They are a blunt instrument trying to hit a highly agile, constantly innovating and ever-changing moving target. Due to their bluntness, and the questions raised as to their ultimate effectiveness, 2020 may see the advent of a new normal, one where cyber diplomacy is in the ascendency, enabling state and private entities to co-operate to develop more creative and effective tools conducive to a globalised and highly agile industry.

**2020 may see the advent of a new normal, one where cyber diplomacy is in the ascendency, enabling state and private entities to co-operate to develop more creative and effective tools conducive to a globalised and highly agile industry.**

## About the authors

**Dr Robert Dewar** is Head of Cyber Security at the Geneva Centre for Security Policy, leading the Centre's cyber security activities. He provides executive education courses on cyber security and defence, the European Union and international relations as well as developing innovative pedagogical approaches to the teaching of cyber security. Robert initiates and engages in international dialogue activities on cyber security and defence and conducts research into cyber security and defence policy, security studies, active and blended learning, the European Union and historical institutionalism. He also specialises in designing, developing and staging policy-based cyber security simulations. Robert has a PhD in EU cyber security policy and an MSc in Global Security from the University of Glasgow, and an MA (Hons.) in Modern History from the University of St. Andrews.

**Ms Ellie Templeton** is a Cyber Security Research Assistant at the Geneva Centre for Security Policy. She has an International Master's Degree in Security, Intelligence and Strategic Studies awarded by the University of Glasgow, Dublin City University and Charles (Prague) University, and an LLB Law Degree from the University of Birmingham, UK. Ellie has an academic background in national and regional law, policy and regulations analysis. Her research has particularly focused on the Europeanisation of security policy within the European Union, cyber security norms and international frameworks, transatlantic intelligence relations and strategy, and conflict studies.

# Endnotes

1. "Shaping the Future of Cybersecurity and Digital Trust > Platforms | World Economic Forum," accessed September 4, 2020, https://www.weforum.org/platforms/shaping-the-future-of-cybersecurity-and-digital-trust

2. Robert Dewar and Ellie Templeton, "The World Health Organisation: The New Cyber Target during a Global Health Crisis and What We Can Learn," www.gcsp.ch, June 3, 2020, https://www.gcsp.ch/global-insights/world-health-organisation-new-cyber-target-during-global-health-crisis-and-what-we

3. Zach Dorfman, "The CIA's New License to Cyberattack," Axios, July 15, 2020, https://www.axios.com/the-cias-new-license-to-cyberattack-43994d91-4717-4af2-b9e4-66aba36d3b0e.html.

4. Brian Barrett, "Chinese Hackers Charged in Decade-Long Crime and Spying Spree," *Wired*, July 21, 2020, https://www.wired.com/story/chinese-hackers-charged-decade-long-crime-spying-spree/

5. "Internet Society Statement on U.S. Clean Network Program | Internet Society," accessed September 4, 2020, https://www.internetsociety.org/news/statements/2020/internet-society-statement-on-u-s-clean-network-program/.

6. David Lektzian and Mark Souva, "Institutions and International Cooperation: An Event History Analysis of the Effects of Economic Sanctions," *Journal of Conflict Resolution* 45, no. 1 (2001): 61.

7. Lance Davis and Stanley Engerman, "History Lessons: Sanctions-Neither War nor Peace," *Journal of Economic Perspectives* 17, no. 2 (2003): 187.

8. Davis and Engerman, 188.

9. Kim Lyons, "Google Parent Alphabet Is Now a $1 Trillion Company," The Verge, January 16, 2020, https://www.theverge.com/2020/1/16/21069458/google-alphabet-trillion-dollar-market-cap-apple-microsoft

10. Lukas Kantor, "Bilderberg Group and Transnational Capitalist Class: Recent Trends in Global Elite Club as Vindication of Neo-Marxism," *Critique* 45, no. 1–2 (April 3, 2017): 183–204, https://doi.org/10.1080/03017605.2016.1268458; Charlie Skelton, "Bilderberg 2018: New Tech Helps Oil the Wheels of the Global Elite," *The Guardian*, June 7, 2018, sec. World news, https://www.theguardian.com/world/2018/jun/07/bilderberg-2018-new-tech-helps-oil-wheels-global-elite

11. In 2019 the European Commission fined Google €1.49 billion for breaching EU antitrust rules. See European Union, "Antitrust: Google Fined €1.49 Billion for Online Advertising Abuse," Text, European Commission - European Commission, accessed September 2, 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770; Nitasha Tiku, "The EU Hits Google With a Third Billion-Dollar Fine. So What? | WIRED," WIRED, March 20, 2019, https://www.wired.com/story/eu-hits-google-third-billion-dollar-fine-so-what/

12. European Commission, "COMMISSION RECOMMENDATION of 26.3.2019 - Cybersecurity of 5G Networks," March 26, 2019, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks

13. "Cyberspace Solarium Commission," accessed August 17, 2020, https://www.solarium.gov/

14. Department of Defense, "Cyber Strategy," 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

15. "Virtual Panel Discussion: Engagement and Competition: China, Technology, and Global Supply Chains | Center for a New American Security," accessed September 3, 2020, https://www.cnas.org/events/virtual-panel-discussion-engagement-and-competition-china-technology-and-global-supply-chains

16. The recommendations and pillars can be found here: "Cyberspace Solarium Commission."

17. "Federal Register: Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment," accessed September 3, 2020, https://www.federalregister.gov/documents/2019/08/13/2019-17201/federal-acquisition-regulation-prohibition-on-contracting-for-certain-telecommunications-and-video

18. A more detailed summary of Section 889 implementation can be found here: "Section 889," 889, accessed August 17, 2020, https://www.ndia.org/policy/section-889

19. This is a brief summarised account. Full details can be found here: "Federal Register :: Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List," accessed September 8, 2020, https://www.federalregister.gov/documents/2020/05/19/2020-10856/export-administration-regulations-amendments-to-general-prohibition-three-foreign-produced-direct.

20. "Announcing the Expansion of the Clean Network to Safeguard America's Assets," *United States Department of State* (blog), accessed August 17, 2020, https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/

21. "The Clean Network - United States Department of State," accessed August 17, 2020, https://www.state.gov/the-clean-network/

22. A definitive is not available, however a U.S. Fact Sheet states such countries include; Albania, Australia, Canada, Czech Republic, Denmark, Estonia, France, Greece, Israel, Japan, Latvia, Norway, Poland, Romania, Slovenia, Sweden, Taiwan, United Kingdom, United States, Vietnam. "The Clean Network Safeguards America's Assets - United States Department of State," accessed September 15, 2020, https://www.state.gov/the-clean-network-safeguards-americas-assets/

23. "Announcing the Expansion of the Clean Network to Safeguard America's Assets."

24. "The Directive on Security of Network and Information Systems (NIS Directive) | Shaping Europe's Digital Future," accessed September 9, 2020, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

25. Erica Moret, Patryk Pawlak, Institute for Security Studies (Paris, *The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?*, 2017, http://www.iss.europa.eu/uploads/media/Brief_24_Cyber_sanctions.pdf

26. Entities sanctioned include Tianjin-based Huaying Haitai, North Korea-based Chosun Expo, and the Centre for Special Technologies, part of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). Individuals sanctioned include affiliated individuals from Russia named Alexey Minin, Aleksei Morenets, Evgenii Serebriakov and Oleg Sotnikov and individuals from China named Gao Qiang and Zhang Shilong. "EU Imposes the First Ever Sanctions against Cyber-Attacks - Consilium," accessed August 21, 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/; European Council, "Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 Implementing Regulation (EU) 2019/796 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States," July 30, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2020.246.01.0004.01.ENG&toc=OJ:L:2020:246:TOC

27. "Press Corner | European Commission," accessed September 4, 2020, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_127

28. "Press Corner | European Commission."

29. "A Europe Fit for the Digital Age | European Commission," accessed September 9, 2020, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

30. "Internet Development, Censorship, and Cyber Crimes in China - Bin Liang, Hong Lu, 2010," accessed September 4, 2020, https://journals.sagepub.com/doi/pdf/10.1177/1043986209350437

31. Jinghan Zeng, Tim Stevens, and Yaru Chen, "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty,'" *Politics & Policy* 45, no. 3 (2017): 432–64

32. "Chinese Law | China: Computer Information Network and Internet Security, Protection and Management Regulations - 1997," accessed September 5, 2020, http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html

33. "Internet Development, Censorship, and Cyber Crimes in China - Bin Liang, Hong Lu, 2010."

34. "Internet Society of China," accessed September 14, 2020, https://www.isc.org.cn/english/Specails/Self-regulation/listinfo-15321.html

35. "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," accessed September 4, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

36. "China's MLPS 2.0: Data Grab or Legitimate Attempt to Improve Domestic Cybersecurity? | CSO Online," accessed September 4, 2020, https://www.csoonline.com/article/3448578/chinas-mlps-20-data-grab-or-legitimate-attempt-to-improve-domestic-cybersecurity.html

37. "China: Navigating the Multi-Level Protection Scheme | DataGuidance," accessed September 4, 2020, https://www.dataguidance.com/opinion/china-navigating-multi-level-protection-scheme

38. "The Huawei Dilemma: Insecurity and Mistrust – The Diplomat," accessed September 4, 2020, https://thediplomat.com/2019/02/the-huawei-dilemma-insecurity-and-mistrust/

39. Jyh-An Lee, "Shifting IP Battlegrounds in the US-China Trade War," *Colum. JL & Arts* 43 (2019): 161.

40. "Strategic Rivalry between United States and China," 5, accessed September 15, 2020, https://www.swp-berlin.org/10.18449/2020RP04/

41. "The Huawei Dilemma: Insecurity and Mistrust – The Diplomat."

42. "Japan Short-Circuits the Tech Exports That Made South Korea Rich - Bloomberg," accessed September 4, 2020, https://www.bloomberg.com/news/articles/2019-12-17/japan-short-circuits-the-tech-exports-that-made-south-korea-rich

43. "Chinese Apps Ban: China Says It Opposes India's Ban on 118 Mobile Apps | International Business News - Times of India," accessed September 4, 2020, https://timesofindia.indiatimes.com/business/international-business/china-says-it-opposes-indias-ban-on-118-mobile-apps/articleshow/77909201.cms

44. Andrew B. Kennedy and Darren J. Lim, "The Innovation Imperative: Technology and US–China Rivalry in the Twenty-First Century," *International Affairs* 94, no. 3 (2018): 558.

45. "Strategic Rivalry between United States and China."

46. "Cyberspace Solarium Commission."

47. A useful aggregator of cyber incidents is the website www.hackmageddon.com

48. "Cyberspace Solarium Commission."

49. "Leaders Seek a Grand Strategy for Cybersecurity | SIGNAL Magazine," accessed September 4, 2020, https://www.afcea.org/content/leaders-seek-grand-strategy-cybersecurity

50. "China May Retaliate Against Nokia and Ericsson If EU Countries Move to Ban Huawei - WSJ," accessed September 4, 2020, https://www.wsj.com/articles/china-may-retaliate-against-nokia-and-ericsson-if-eu-countries-move-to-ban-huawei-11595250557

51. Moret, Pawlak, and Institute for Security Studies (Paris, *The EU Cyber Diplomacy Toolbox*).

52. "Cyberspace Solarium Commission."

53. Jack Linchuan Qiu, "Virtual Censorship in China: Keeping the Gate Between the Cyberspaces," *International Journal of Communications Law and Policy* 4 (2000).

54. "China's Internet Industry Calls for Self-Discipline," accessed September 15, 2020, http://www.china.org.cn/english/2002/Mar/29518.htm

55. "Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals | Government of the Czech Republic," accessed September 3, 2020, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/

56. James Andrew Lewis, "Criteria for Security and Trust in Telecommunications Networks and Services," CSIS Working Group on Trust and Security in 5G Networks: Criteria for Security and Trust in Telecommunications Networks and Services, June 13, 2020, https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services

57. "China: Navigating the Multi-Level Protection Scheme | DataGuidance."

58. Practical Law, "Communications: Regulation and Outsourcing in China," accessed September 15, 2020, https://signon.thomsonreuters.com/?productid=PLCUK&viewproductid=UKPL&lr=0&culture=en-GB&returnto=https%3a%2f%2fuk.practicallaw.thomsonreuters.com%2fCosi%2fSignOn%3fredirectTo%3d%252fw-013-7289%253ftransitionType%253dDefault%2526contextData%253d(sc.Default)%2526firstPage%253dtrue&tracetoken=0915201101060Ep-ZBQbbdkX62To1aDwYOjcH3llcjai4vVj4h_YxITrWEr5qgqTTtzCwk-b2ctX5XCo9UJros2gebzr2TdZVIaVOKsdC_am_EQB6QxTlVzof-2Y_TD-jU-cpA5c9vztm7XgNvg0A_XEoe9cuX22nwzRAs_1zG_zaUpD9_cA-FEefn2PGa6Vu482OtH8WNUxvO8UKnhqCcrxv2fKUn3gftbexGRm-mUOUotKDNITcI8FLZ5h50AWePXx3BQ1w-05N9ItcnTfpxePTB8iPJG-Ja4GECvZ25PKJhRj4bxvlMFGY9-SRrxVidh7Ock2c0WocMNTqLCvxcvK-FM527aRpbxwSerUfeT_Fn6MK1NXRmeFgEv77YNZMFjZ6La2-PafkES-2jEY7&bhjs=0

59. Antonio Douglas, "How Companies Are Reacting to China's New Data Security Scheme," *China Business Review* (blog), April 3, 2020, https://www.chinabusinessreview.com/why-companies-are-still-reluctant-to-file-in-chinas-new-data-security-scheme/

60. Lewis, "Criteria for Security and Trust in Telecommunications Networks and Services."

61. "Huawei to Be Removed from UK 5G Networks by 2027 - GOV.UK," accessed September 6, 2020, https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027

62. "Huawei: Why Is It Being Banned from the UK's 5G Network? - BBC News," accessed August 18, 2020, https://www.bbc.co.uk/news/newsbeat-47041341

63. For example, Huawei is one of the largest corporate investors, spending over 14% of its revenue on R&D in 2018 and has 16 dedicated international R&D centres. It has recently quadrupled its personnel in Russian centres. "Why Is Huawei Spending $15bn on R&D? | GovInsider," accessed September 4, 2020, https://govinsider.asia/connected-gov/huawei-15-billion-research-development-spending/

64. Alexander Gabuev, "Huawei's Courtship of Moscow Leaves West in the Cold," Financial Times, accessed September 4, 2020, https://www.ft.com/content/f36a558f-4e4d-4c00-8252-d8c4be45bde4

65. "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies | U.S. Department of Commerce," accessed September 8, 2020, https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts

66. "Huawei Sanctions: Bad for Telecoms, Global Semiconductors and the US Economy," accessed September 4, 2020, https://www.strategyanalytics.com/strategy-analytics/blogs/components/rf-wireless/rf-and-wireless/2020/06/04/huawei-sanctions-bad-for-telecoms-global-semiconductors-and-the-us-economy

67. "China Threatens to Place Apple, Boeing, and Other U.S. Firms on 'Unreliable Entities' List | National Review," accessed September 7, 2020, https://www.nationalreview.com/news/china-threatens-to-place-apple-boeing-and-other-u-s-firms-on-unreliable-entities-list/

68. "Graham Webster on TikTok, Huawei, and the US-China Tech Clash – The Diplomat," accessed September 4, 2020, https://thediplomat.com/2020/07/graham-webster-on-tiktok-huawei-and-the-us-china-tech-clash/

69. "Huawei Sanctions: Bad for Telecoms, Global Semiconductors and the US Economy."

70. "U.S. Urges EU to Use 5G by Ericsson, Nokia, Samsung, Seen on Par with Huawei | Reuters," accessed September 8, 2020, https://uk.reuters.com/article/uk-telecoms-5g-huawei-portugal/u-s-urges-eu-to-use-5g-by-ericsson-nokia-samsung-seen-on-par-with-huawei-idUKKBN20D1NL

71. "Huawei Sanctions: Bad for Telecoms, Global Semiconductors and the US Economy."

72. "Virtual Panel Discussion: Engagement and Competition: China, Technology, and Global Supply Chains | Center for a New American Security."

73. "The EU Toolbox for 5G Security | Shaping Europe's Digital Future," accessed September 3, 2020, https://ec.europa.eu/digital-single-market/en/news/eu-toolbox-5g-security

74. "Cyberspace Solarium Commission."

75. Paul Schwartz, "Data Localization Under the CLOUD Act and the GDPR," *Computer Law Review International* 1 (n.d.): 1–10.

76. "The European Court of Justice Overrides Privacy Shield. Implications for Businesses. | Ashurst," accessed September 7, 2020, https://www.ashurst.com/en/news-and-insights/legal-updates/the-european-court-of-justice-overrides-privacy-shield---implications-for-businesses/

77. "U.S. Companies Can Work with Huawei on 5G, Other Standards: Commerce Department - Reuters," accessed September 4, 2020, https://www.reuters.com/article/us-usa-china-huawei-tech-exclusive/us-companies-can-work-with-huawei-on-5g-other-standards-commerce-department-idUSKBN23M2DF

78. "Internet Society Statement on U.S. Clean Network Program | Internet Society"; "Cyber Chief Warns of East-West Split over the Internet | The Union Journal," accessed September 4, 2020, https://theunionjournal.com/cyber-chief-warns-of-east-west-split-over-the-internet/

79. "Global Initiative on Data Security," accessed September 14, 2020, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml

80. "China Launches Global Data Security Initiative, Respects Data Sovereignty - Global Times," accessed September 14, 2020, https://www.globaltimes.cn/content/1200228.shtml

81. "Global Initiative on Data Security."

82. "Global Commission on the Stability of Cyberspace," accessed September 14, 2020, https://cyberstability.org/

83. "What the Digital Geneva Convention Means for the Future of Humanitarian Action," *UNHCR Innovation* (blog), June 25, 2017, https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/

84. "Huawei: Why Is It Being Banned from the UK's 5G Network? - *BBC News*."

85. "Summary of the NCSC Analysis of May 2020 US Sanction," accessed August 17, 2020, https://www.ncsc.gov.uk/report/summary-of-ncsc-analysis-of-us-may-2020-sanction

86. Leo Kelion, "Huawei: What Would Happen If the UK Ditched the Chinese Firm?," *BBC News*, May 25, 2020, sec. Technology, https://www.bbc.co.uk/news/technology-52797859

87. Sam Byford, "US Sanctions Make Huawei More of a Security Risk, Says Leaked UK Report," *The Verge*, July 6, 2020, https://www.theverge.com/2020/7/6/21314340/huawei-5g-networks-security-risk-us-uk

88. "Leaders Seek a Grand Strategy for Cybersecurity | SIGNAL Magazine."

89. Anecdotal evidence is already emerging of third-party vendors using complicated and convoluted supply networks as a means to circumvent these regulations in order to secure components that are only produced by proscribed vendors. Future analyses will be able to examine these in greater detail.

90. Tambiama Madiega, "Digital Sovereignty for Europe: Towards a More Resilient EU" (European Parliamentary Research Service, July 2020).

91. Simon J. Evenett, "The Impact of Economic Sanctions on South African Exports," *Scottish Journal of Political Economy* 49, no. 5 (2002): 557.

92. "Shaping the Future of Cybersecurity and Digital Trust > Platforms | World Economic Forum."

93. "Many Cyberspace Solarium Commission Recommendations Expected to Become Federal Law | CSO Online," accessed September 3, 2020, https://www.csoonline.com/article/3568450/many-cyberspace-solarium-commission-recommendations-expected-to-become-federal-law.html

94. European Commission, "5G Security: Member States Report on Progress on Implementing the EU Toolbox and Strengthening Safety Measures," July 24, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1378

95. "China Launches Initiative to Set Global Data-Security Rules - WSJ," accessed September 11, 2020, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974

GCSP
Geneva Centre for Security Policy

# Cyber Security Policy Brief

**Geneva Centre for Security Policy - GCSP**
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
CH-1211 Geneva 1
Tel: + 41 22 730 96 00
Fax: + 41 22 730 96 49
e-mail: info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-113-3