# 1AC

## 1AC — KU HW

### 1AC — Innovation

#### Advantage 1 is Innovation —

#### Standards-Setting Organizations [SSO’s] are industry members who jointly establish standards for information tech defined by the adoption of standard-essential patents [SEP’s], which are licensed to companies who wish to implement the tech in their product, called implementers, on Fair, Reasonable, and Non-Discriminatory [FRAND] terms. Current standards promote price gouging, FRAND enforcement is critical.

Melamed & Shapiro 18, \*A. Douglas Melamed is Professor of the Practice of Law at Stanford Law School; \*Carl Shapiro is the Transamerica Professor of Business Strategy at the Haas School of Business at the University of California at Berkeley; (May 2018, “How Antitrust Law Can Make FRAND Commitments More Effective”, https://www-cdn.law.stanford.edu/wp-content/uploads/2018/05/How-Antitrust-Law-Can-Make-FRAND-Commitments-More-Effective.pdf)

I. Standard Setting and the Competitive Process

The fundamental economics in the information technology sector, driven by network effects, implies that there is enormous value associated with establishing compatibility standards. Popular standards include the mobile broadband standards used in cell phones, which are established by the 3rd Generation Partnership Project (3GPP), and the Wi-Fi technology for wireless local area networks, which is enabled by the 802.11 standard established by the Institute of Electrical and Electronics Engineers (IEEE).4

There are many SSOs, and their rules and procedures differ considerably. In addition to IEEE, leading SSOs include the International Organization for Standardization (ISO), the International Telecommunication Union (ITU), the European Telecommunications Standards Institute (ETSI), the Internet Engineering Task Force (IETF), and the World Wide Web Consortium (W3C).5 SSOs generally establish standards by holding a series of committee meetings among industry participants. These meetings culminate in a vote on a technical specification that describes what features or attributes a product must have in order to comply with the standard. Most SSOs are open to all industry participants and seek to operate on a consensus basis, applying certain voting rules. SSOs do not normally engage in patent licensing, nor do they specify how patent royalties will be divided up among patent holders. They leave that to their members, which in some cases form patent pools to address these issues.6

SSOs adopt specific policies relating to intellectual property rights (IPRs).7 These IPR policies are generally intended to enable the SEP holders to obtain reasonable royalties for licensing their patents, while prohibiting them from charging excessive royalties after other industry participants have committed to the standard. At that point, firms committed to implementing the standard— which we call “implementers”—would find it very costly to avoid using the patented technology. For this purpose, most SSOs require SEP owners to license their SEPs on FRAND terms.8

FRAND policies are especially necessary because negotiations between SEP holders and implementers generally take place only after the implementers have used and infringed the technologies claimed by the SEPs. Standards involving information and communications technology can involve hundreds or even thousands of SEPs, many with uncertain boundaries for infringement. In addition, a time lag exists between patent application and patent issuance. For these and other reasons, it is impractical for implementers to enter into negotiations for patent licenses with all SEP owners prior to the establishment of a standard and to their implementation of it.9

The fact that patent negotiations generally do not take place until after implementers have used and infringed the technologies has several critical implications. First, at the time of negotiation, implementers are locked into the standard and the technologies claimed by the SEPs—that is, the cost to switch to an alternative technology or standard at that point—ex post—is much greater than it was ex ante, before the patented technology was first included in the standard. Ex post, the patent holder is no longer competing to have its technology included in the standard, nor is it competing to have implementers of the standard use its technology. Instead, because the patent holder owns an asset that is essential to the standard, implementers have no choice but to use the patented technology.

If the standard is commercially successful, implementers are willing to pay a much larger royalty for use of the patented technology than they would have paid ex ante, when the SEP holder faced competition from other technologies. In these circumstances, the SEP holder can be said to have obtained monopoly power in the market in which the patented technology is licensed for use in implementing the standard.10

Second, because of lock-in and the implementer’s ongoing infringement, the potential for litigation looms large in licensing negotiations. In effect, the parties are negotiating about how to settle an infringement suit, and that negotiation is heavily influenced by their predictions as to what the court will do if they cannot agree. This situation is not unique to SEPs; it arises frequently when firms are faced with patent infringement claims for products they have independently developed or technologies they have inadvertently infringed. Patent law addresses such instances by specifying that patent holders are entitled to “reasonable royalties,” defined as the royalties that the parties would have negotiated prior to the infringement and thus prior to lock-in.11 Those hypothetical ex ante royalties reflect the market value of the patent license. Notwithstanding the law’s embrace of this principle, however, as a practical matter, patent holders are generally able to recover more than the ex ante value of the patent when litigation occurs after the implementers are locked in. Further, negotiations in the shadow of litigation after lock-in tend to result in royalties in excess of the ex ante or market value of the patented technology.12

Third, the shadow of litigation is particularly problematic in the communications and technology sector, in which products typically include hundreds or thousands of patented technologies. A court-ordered injunction involving such products would deprive the implementer of not only the value of the technology covered by the patent-in-suit, but also the value of the entire product.13 Implementers that are forced to bear the risk of an injunction are thus induced to agree to royalties greater than those that would be appropriate if only the value of the patented technology were at stake. Those royalties systematically provide SEP holders with excessive compensation in comparison with the benchmark of ex ante royalties.

These implications of lock-in and ex post dealings are well-understood: they represent an example of the general concept of lock-in and opportunism developed by Oliver Williamson.14 The Federal Circuit has also recognized the market distortions caused by the inclusion of patented technologies in public standards and the resulting danger of patent holdup involving SEPs.15

For these and other reasons, the SEP holder has ex post monopoly power that, if left unchecked, would enable it to obtain royalties far in excess of the royalties that it could earn in a competitive market.16 To address this common problem and limit ex post opportunism by SEP holders, SSOs typically require participants that own SEPs to make certain FRAND commitments. In particular, by requiring a commitment to license on “fair and reasonable” terms, the FRAND requirement aims to prevent, or at least reduce, the extent of monopoly pricing by SEP holders. And by requiring a commitment to license on “nondiscriminatory” terms, the FRAND requirement can prevent SEP holders from extracting monopoly premiums by selective licensing or, more important, migrating their monopoly power from the FRAND-regulated market to unregulated standard-implementing product markets by licensing to only one or a few implementers or licensing to selected implementers on discriminatorily favorable terms.

#### Patent holdup is accentuated by the Ninth Circuit’s recent decision in *FTC v. Qualcomm* that permits ICT firms to engage in innovation-stifling conduct with antitrust impunity.

Moss 20, \*Alex Moss is a Staff Attorney on EFF’s intellectual property team, before joining EFF, Alex practiced complex commercial litigation at Sullivan & Cromwell LLP in New York and Durie Tangri LLP in San Francisco; (August 26th, 2020, “Throwing Out the FTC's Suit Against Qualcomm Moves Antitrust Law in the Wrong Direction”, https://www.eff.org/deeplinks/2020/08/throwing-out-ftcs-suit-against-qualcomm-moves-antitrust-law-wrong-direction)

Standards can enhance competition and consumer choice, but they also massively inflate the value of patents deemed essential to the standard, and give their owners the power to sue companies that implement the standard for money damages or injunctions to block them from using their SEPs. When standards cover critical features like wireless connectivity, SEP owners wield a huge amount of “hold-up” power because their patents allow them to effectively block access to the standard altogether. That lets them charge unduly large tolls to anyone who wants to implement the standard.

To minimize that risk, standard-setting organizations typically require companies that want their patented technology incorporated into a standard to promise in advance to license their SEPs to others on fair, reasonable, and non-discriminatory (FRAND) terms. But that promise strikes at a key tension between antitrust and patent law: patent owners have no obligation to let anyone use technology their patent covers, but to get those technologies incorporated into standards, patent owners usually have to promise that they will give permission to anyone who wants to implement the standard as long as they pay a reasonable license fee.

Qualcomm is one of the most important and dominant companies in the history of wireless communication standards. It is a multinational conglomerate that has owned patents on every major wireless communication standard since its first CDMA patent in 1985, and it participates in the standard-setting organizations that define those standards. Qualcomm is somewhat unique in that it not only licenses SEPs, but also supplies the modem chips used by a wide range of devices. These include chips that implement wireless communication standards, which lie at the heart of every mobile computing device.

Although Qualcomm promised to license its SEPs (including patents essential to CDMA, 3G, 4G, and 5G) on FRAND terms, its conduct has to many looked unfair, unreasonable, and highly discriminatory. In particular, Qualcomm has drawn scrutiny for bundling tens of thousands of patents together—including many that are not standard-essential—and offering portfolio-only licenses no matter what licensees actually want or need; refusing to sell modem chips to anyone without a SEP license and threatening to withhold chips from companies trying to negotiate different license terms; refusing to license anyone other than original-equipment manufacturers (OEMs); and insisting on royalties calculated as a percentage of the sale price of a handset sold to end users for hundreds of dollars, despite the minimal contribution of any particular patent to the retail value.

In 2017, the U.S. Federal Trade Commission [sued](https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-qualcomm-monopolizing-key-semiconductor-device-used) Qualcomm for violating both sections of the Sherman Antitrust Act by engaging in a number of anticompetitive SEP licensing practices. In May 2019, the U.S. District Court for the Northern District of California agreed with the FTC, identifying numerous instances of Qualcomm’s unlawful, anticompetitive conduct in a comprehensive [233-page opinion](https://www.eff.org/document/ftc-v-qualcomm-district-court-opinion). We were pleased to see the FTC take action and the district court credit the overwhelming evidence that Qualcomm’s conduct is corrosive to market-based competition and threatens to cement Qualcomm’s dominance for years to come.

But this month, a panel of judges from the Court of Appeals for the Ninth Circuit unanimously [overturned](https://www.eff.org/document/ninth-circuit-opinion-ftc-v-qualcomm) the district court’s decision, reasoning that Qualcomm’s conduct was “hypercompetitive” but not “anticompetitive,” and therefore not a violation of antitrust law. To reach that result, the Ninth Circuit made the patent grant more powerful and antitrust law weaker than ever.

According to the Ninth Circuit, patent owners don’t have a duty to let anyone use what their patent covers, and therefore Qualcomm had no duty to license its SEPs to anyone. But that framing requires ignoring the promises Qualcomm made to license its SEPs on reasonable and non-discriminatory terms—promises that courts in this country and around the world have consistently enforced. It also means ignoring antitrust principles like the essential facilities doctrine, which limits the ability of a monopolist with hold-up power over an essential facility (like a port) to shut out rivals. Instead, the Ninth Circuit held rather simplistically that a duty to deal could arise only if the monopolist had provided access, and then reversed its policy.

But even when Qualcomm restricted its licensing policies in critical ways, the Ninth Circuit found reasons to approve those restrictions. For example, Qualcomm stopped licensing its patents to chip manufacturers and started licensing them only to OEMs. This had a major benefit: it let Qualcomm charge a much higher royalty rate based on the high retail price of the end user devices, like smartphones and tablets, that OEMs make and sell. If Qualcomm had continued to license to chip suppliers, its patents would be “exhausted” once the chips were sold to OEMs, extinguishing Qualcomm’s right to assert its patents and control how the chips were used.

Patent exhaustion is a century-old doctrine that protects the rights of consumers to use things they buy without getting the patent owner’s permission again and again. Patent exhaustion is important because it prevents price-gouging, but also because it protects space for innovation by letting people use things they buy freely, including to build innovations of their own. The doctrine thus helps patent law serve its underlying goal—promoting economic growth and innovation. In other words, the doctrine of exhaustion is baked into the patent grant; it is not optional. Nevertheless, the Ninth Circuit wholeheartedly approved of Qualcomm’s efforts to avoid exhaustion—even when that meant cutting off access to previous licensees (chip-makers) in ways that let Qualcomm charge far more in licensing fees than its SEPs could possibly have contributed to the retail value of the final product.

It makes no sense that Qualcomm could contract around a fundamental principle like patent exhaustion, but at the same time did not assume any antitrust duty to deal under these circumstances. Worse, it’s harmful for the economy, innovation, and consumers. Unfortunately, the kind of harm that antitrust law recognizes is limited to harm affecting “competition” or the “competitive process.” Antitrust law, at least as the Ninth Circuit interprets it, doesn’t do nearly enough to address the harm downstream consumers experience when they pay inflated prices for high-tech devices, and miss out on innovation that might have developed from fair, reasonable, and non-discriminatory licensing practices.

We hope the FTC sticks to its guns and asks the Ninth Circuit to go en banc and reconsider this decision. Otherwise, antitrust law will become an even weaker weapon against innovation-stifling conduct in technology markets.

#### Weakened antitrust enforcement emboldens firms to follow Qualcomm’s lead, which collapses FRAND integrity.

Hovenkamp 20, \*Herbert J. Hovenkamp is James G. Dinan University Professor at the University of Pennsylvania Law School and the Wharton School of the University of Pennsylvania; (2020, “FRAND and Antitrust”, <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3095&context=faculty_scholarship>)

While the FRAND process has been highly productive, it is also fragile. Firms are tempted to make commitments at the beginning when the incentive to join is large, but renege on them later when they can profit by doing so. At least in this particular case, private FRAND enforcement had not worked very well. Qualcomm had been able to violate FRAND commitments in order to exclude rivals and obtain higher royalties than FRAND would permit, largely with impunity. Other firms will very likely follow Qualcomm’s lead. If that happens the FRAND system will fall apart, doing irreparable injury to the modern wireless telecommunications network or, at the very least, diminishing the leadership role of the United States in preserving effective network competition.

While governments can be heavily involved in standard set-ting,9 the implementation of technical standards in information technologies is largely the work of private actors. Government involvement is limited mainly to enforcement of contract, intellectual property, or antitrust law. As private actors, those involved in standard setting or compliance are fully subject to the federal antitrust laws.

This Article addresses one question: when is an SSO participant’s violation of a FRAND commitment an antitrust violation, and if it is, of what kind and what are the implications for remedies? It warns against two extremes. One is thinking that any violation of a FRAND commitment is an antitrust violation as well. In the first instance FRAND obligations are contractual, and most breaches of contract do not violate any antitrust law. The other extreme is thinking that, because a FRAND violation is a breach of contract, it cannot also be an antitrust violation. The question of an antitrust violation does not de-pend on whether the conduct breached a particular agreement but rather on whether it caused competitive harm. This can happen because the conduct restrained trade under section 1 of the Sherman Act, was unreasonably exclusionary under section 2 of the Sherman Act, or amounted to an anticompetitive condition or understanding as defined by section 3 of the Clay-ton Act.10 The end goal is to identify practices that harm com-petition, thereby injuring consumers.

The Ninth Circuit’s Qualcomm decision will make antitrust violations in the context of FRAND licensing much more difficult to prove, even in cases where anticompetitive behavior and consumer harm seem clear.11 Indeed, in this case the court itself acknowledged the harm to consumers but appeared to think that they were not entitled to protection.12 If this decision stands, FRAND obligations will to a larger extent have to be settled through private litigation and the federal antitrust enforcement agencies will have a diminished role. Anticompetitive behavior by one firm that is not effectively disciplined will lead others to do the same thing.

#### A trusted and credible system for ICT innovation is critical to rapid tech diffusion and economic growth---absent FRAND, the system will collapse.

Bauer et al. 17, \*Matthias Bauer is Senior Economist at ECIPE; \*Fredrik Erixon is a Swedish economist and writer. He has been the Director of the European Centre for International Political Economy (ECIPE) ever since its start in 2006; (October 2017, “Standard Essential Patents and the Quest for Faster Diffusion of Technology”, https://ecipe.org/publications/standard-essential-patents/)

It is easy to take a pessimistic view about whether the system will break. If the current trend continues, the system is likely to break at some point for the simple reason that companies will not trust it anymore. The series of legal disputes witnessed over the past years – sometimes referred to as the “smartphone patent wars” – has been fodder for a pessimistic reading of “the two tales of SEPs”. While it is common in the business world that disputes over patents and licenses are settled in courts, various SEP disputes have revealed problematic aspects of the SEP market that are different from those disputes that follow the normal stream of business and contracts. Often, the SEP disputes are less concerned about the rights and boundaries of patents, and more about antitrust limits to market behavior: they concern market abusive practices and restrictions to competition as much as they are about intellectual property.

If the SEP system actually does break at some point, the consequences would be felt throughout the economy. SEPs have been a critical part of the ICT revolution. SEPs have allowed for the fast rates of innovation diffusion that the world has witnessed over the past quarter of a century. All the computer and Internet related products and services that people are now dependent upon for their private and professional lives are intricate webs of intellectual property. As many as 250,000 patents can be used to claim ownership of some technical specification or design element in a single smartphone (NYT 2012). A laptop, suggests one calculation, implements more than 250 interoperability standards (Biddle et al. 2010), and the number of SEP holders for 3G and 4G standards grew from 2 in 1994 to 130 in 2013 while the number of SEPs rose from fewer than 150 in 1994 to more than 150,000 in 2013 (Galetovic and Gupta 2016). The standardization-body ETSI has registered more than 150,000 declarations of SEPs from companies, and ETSI is just one of many bodies in the world of ICT standardization. For the 3G standard, the same body has about 24,000 patents that have been declared essential. Now, with the economy yet again on the threshold of big technological change, a trusted and credible system for creators and users of technology to standardize proprietary technology would be a boon for innovation, interoperability and – ultimately – the consumers.

And there are reasons for optimism. Although many of the problems in the SEP regimes need to be addressed, the numbers above indicate that the SEP system is in fact attractive to patent holders and SEP implementers. It is easy to see why: neither holders nor implementers are presented with alternative options that on the face of it would be far more profitable for them. In other words, there simply would not be as many patents declared as essential if both creators and users of technology believed the SEP system worked to their disadvantage or was grossly unfair. While the reality for some companies may be that legal disputes and unpredictability prompt them to find other ways than SEPs to get access to key technologies for their products, it remains the case that most stakeholders have strong economic incentives to maintain a balanced SEP system that is trusted.

First, standard essential patents are an asset for creators of technology because, by becoming essential to a standard, their volumes of sales for technologies that users value rise significantly. As many holders want to raise more revenues for their SEPs and – ideally – have the freedom to contract with buyers on their terms, they can expand their customer base when they agree to sell patented technology in accordance with a set of rules that are designed to prevent SEP holders exploiting the weakness of a customer that has grown dependent on having access to their technology.

Second, SEPs are hugely beneficial also to those that buy the licenses – the implementers or users. Through the SEP system, they can access technologies that are interoperable and work with different products and functionalities – and they can do it under conditions that, if history is a guide, in most cases give them stable and predictable terms of contract. As a consequence, both creators and users can focus on their competitive advantages and profit on the economies of scale and specialization. Downstream firms do not need to develop their own upstream technology and upstream firms do not need to package their technologies in end-customer products in order to make their products valuable.

Third, standard-setting organisations (SSOs) also have a big stake in an SEP system that works well – and, like creators and users of technology, they would stand to lose significantly if the SEP system were to collapse.

Lastly, the biggest beneficiaries are individual consumers – those who buy the end products using FRAND-conditioned SEPs. The advent of SEPs and the rules represented by FRAND have enabled a development of fast technology creation and contributed to the rapid diffusion in ICT goods and ICT-based services. The SEP system has also allowed for new competition, both between existing technologies and brands, and from new ones that have stepped into the market with the ambition to disrupt it, again to the benefit of the consumer. It is difficult to imagine that the ICT and digital development would have been as fast as it has been if SEPs had not been a central feature of the market.

The changing fortunes of companies operating in the cellular and smartphone market would not have been possible if there had not been an SEP system that supported competition. Now that the world economy is on the doorstep of new innovations that are dependent on a great number of input technologies – e.g. the Internet-of-Things, transport connectivity and intelligent vehicles – it is crucially important for the consumer that a balanced and functioning SEP system is maintained and that actors in the system converge towards it – which would ultimately meet their economic interests.

#### ICT innovation is key to post-COVID economic recovery and long-term growth.

van Ark 21, \*Bart van Ark is a Senior Advisor of the Economy, Strategy and Finance (ESF) Center at The Conference Board; Bart van Ark, \*Klaas de Vries is an economist with The Conference Board; \*Abdul Erumban is an assistant professor at the University of Groningen, The Netherlands and a senior research fellow at The Conference Board; (2021, “HOW TO NOT MISS A PRODUCTIVITY REVIVAL ONCE AGAIN”, https://sci-hub.se/10.1017/nie.2020.49)

Introduction

As the global economy has entered recession in 2020, triggered by the COVID-19 pandemic, the human casualties, and economic damage are perceived to be very large. Even as the health crisis will gradually become manageable, the impact on economic growth can be long-lasting and the recovery path can take several years. In particular, growth drivers such as the pace of job creation, income generation and investment may take several years to get back to pre-crisis trends. Initially the productivity of those growth drivers may be of less concern as the mantra of ‘we’ll do what it takes to avoid worse’ is predominant in this phase of the crisis.

However, once the recovery gets underway the productive use of resources is key to sustained growth. While we do not ignore the short-term challenges of the economic recovery, our primary focus in this paper is on the productivity puzzle from a long-term perspective. Productivity is driven by technological change and innovation which, in turn, depends on investment in human and physical capital as well as in other ‘missing capitals’ often referred to as intangible assets. Indeed, those investments create a positive feedback effect, as the productivity it generates also helps to make more efficient usage of scarce resources in the future. When properly measured and valued, productivity also provides a critical yardstick to realise a fairer distribution of the gains from economic growth to those who bring the resources to bear. It thereby creates the incentives for people to produce and business to invest helping to drive economic growth and raise living standards.

Unfortunately, in the aftermath of the global financial crisis of 2008/2009, many economies around the world, especially advanced economies, have failed to recharge the economy by powering productivity as the key source of growth in the long term. Indeed the latest update of The Conference Board Total Economy Database (July 2020) points at significant weakening in labor productivity growth in Europe up to 2019 (figure 1a–c). While the United States experienced somewhat faster productivity growth from 2017 to 2019 than the Euro Area and the United Kingdom, it still has not recovered to the rates of productivity growth from before the global financial crisis either.

The slowdown in productivity growth over the past 15 years has been well documented. There are multiple causes including an exhaustion of catch-up potential in emerging markets impacting economies along entire global value chains, and the drag from the global financial crisis because of low demand and weak investment, too low interest rates causing misallocations an overreliance on cheap labor, and failing fiscal policies (Bauer et al., 2020; Cette et al., 2016; Crafts, 2018; Dieppe, 2020; Fernald et al., 2017; Syverson, 2016).1 Technical measurement issues regarding inputs and outputs may have played a role as well.

In our earlier work we have stressed the importance of time lags in the adoption of new technologies, and in particular the complexity in generating productivity growth from the latest round of new digital technologies since the early 2010s, including the move toward mobile, ubiquitous access to broadband, the rise of cloud storage and advances in artificial intelligence (AI) and robotics (van Ark, 2016a, 2016b; van Ark and O’Mahony, 2016; van Ark et al., 2016).

While the first priority for economic recovery from the COVID-19 crisis is to restore jobs, it is important that any employment-intensive growth path does go together with a productivity revival. In this paper, we argue that it is possible to avoid another productivity slowdown. Underneath the aggregate figures, there is evidence pointing toward a possible tipping point at which many advanced economies may expect to see more widespread impacts from the adoption and absorption of digital technology on productivity and GDP growth.

In Section 2 we review the latest literature on the productivity impacts of general purpose technologies (GPTs), including the notion of time lapses through which digital technologies result in faster productivity growth. We also look at patterns by which innovation and productivity effects GPTs emerge across industries and disperse across the economy. We explain why the New Digital Economy (NDE) is especially characterised by long lag effects.

In Section 3 we provide an empirical analysis of productivity growth by industry data to observe whether we can detect a distinct pattern across groups of industries pointing to a structural improvement in recent years. We use a taxonomy on digital intensity by industry which was recently developed by the Organisation for Economic Co-operation and Development (OECD) (Calvino et al., 2018), showing that the most digital-intensive industries have experienced a relatively strong performance in terms of labor productivity growth since 2007 and especially since 2013.

In Section 4 of the paper, we discuss the connection between labor and skills in the digital economy, which we believe provides the key to a productivity revival. We developed a new metric on innovation competencies by occupation on the basis of data from the O\*Net database on occupation-specific descriptors in the United States (Hao et al., 2018). When applied to the United Kingdom, we find that innovation competencies point at stronger productivity effects by industry.

In Section 5 we focus on how productivity has been behaving in the short-term during the COVID-19 recession. In particular, we address the potential trade-offs between traditional pro-cyclical recovery effects and scarring effects the recession leaves, especially on the labor market. We argue that increased adoption and usage of digital technologies during the COVID-19 crisis may create a positive productivity effect. In the final section, Section 6, we will review our hypothesis that a productivity revival could be imminent in the light of the recovery from the COVID-19 crisis. In order not to miss this opportunity again, as happened a decade ago, we argue that a coordinated effort from business and policy is needed, and has to be delivered in such a way that the gains from productivity will be more widespread and such that those who provide the resources for growth are incentivised to deliver them in an efficient way.

2. The productivity paradox of the New Digital Economy

It is well known that General Purpose Technologies (GPTs), defined as new methods of producing and inventing new goods and services which are important enough to have a long-term aggregate impact on the economy, can take a significant amount of time to translate to faster productivity growth at the aggregate level of the economy. This is inherent to the three critical characteristics of a GPT as identified by Bresnahan and Trajtenberg (1995).2

1. Pervasiveness –The GPT should spread to most sectors.

2. Improvement –The GPT should get better over time and, hence, should keep lowering the costs of its users.

3. Innovation spawning –The GPT should make it easier to invent and produce new products or processes.

Historical analysis has focussed on productivity trends in previous technology phases (Bakker et al., 2019; Crafts, 2004). Recent literature has shown that the information and communication technology (ICT) revolution of the past 50 years can be characterised as a GPT and doesn’t pale with previous GPTs such as steam technology, electricity and the combustion engine. For example, Hempell (2005) concludes that ‘investment in information and communication technologies (ICT) are closely linked to complementary innovations and are most productive in firms with experience from earlier innovations’. In a more recent analysis of the evolution of the Internet, Simcoe (2015) argues that the modularity of the internet has prevented a fall in return to investments in innovation by ‘facilitating low-cost adaptation of a shared general-purpose technology to the demands of heterogeneous applications’. In a review of the data, Liao et al. (2016) conclude that:

‘...ICT investment does contribute to productivity but not in the usual manner –we find a positive (but lagged) ICT effect on technological progress. We argue that for a positive ICT role on growth to actually take place, a period of negative relationship between productivity and ICT investment together with ICT-using sectors’ capacity to learn from the embodied new technology was crucial. In addition, it took a learning period with appropriate complementary co-inventions for the new ICT-capital to become effective and its gains to be realised. Our findings provide solid, further empirical evidence to support ICT as a general purpose technology’.

#### Growth solves nuclear war.

Henricksen 17, \*Thomas H., emeritus senior fellow at the Hoover Institution; (March 23rd, 2017, “Post-American World Order,” Hoover Institution, <http://www.hoover.org/research/post-american-world-order>)

What Is To Be Done?

The first marching order is to dodge any kind of perpetual war of the sort that George Orwell outlined in  “1984,” which engulfed the three super states of Eastasia, Eurasia, and Oceania, and made possible the totalitarian Big Brother regime. A long-running Cold War-type confrontation would almost certainly take another form than the one that ran from 1945 until the downfall of the Soviet Union.

What prescriptions can be offered in the face of the escalating competition among the three global powers? First, by staying militarily and economically strong, the United States will have the resources to deter its peers’ hawkish behavior that might otherwise trigger a major conflict. Judging by the history of the Cold War, the coming strategic chess match with Russia and China will prove tense and demanding—since all the countries boast nuclear arms and long-range ballistic missiles. Next, the United States should widen and sustain willing coalitions of partners, something at which America excels, and at which China and Russia fail conspicuously.

There can be little room for error in fraught crises among nuclear-weaponized and hostile powers. Short- and long-term standoffs are likely, as they were during the Cold War. Thus, the playbook, in part, involves a waiting game in which each power looks to its rivals to suffer grievous internal problems which could entail a collapse, as happened to the Soviet Union.

Some Chinese and Russian experts predict grave domestic problems for each other. They also entertain similar thoughts about the United States, which they view as terminally decadent and catastrophically polarized over politics, ethnicity, and the future direction of the country. So, the brewing three-way struggle also involves a systemic contest, which will test the competitors’ economic and political institutions.

At this juncture, the world is entering a standoff among the three great and several not-so-great powers. Averting war, while defending our interests, will prove a challenge, calling for deft policy, political endurance, and economic growth, as well as sufficient military force to keep at bay aggressive states or prevail over them if ever a war breaks out.

#### Absence of domestic 5G competition cedes leadership in technical standards to China.

Duan 19, \*Charles Duan is a senior fellow and associate director of tech & innovation policy at the R Street Institute, where he focuses his research on intellectual property issues; (February 5th, 2019, “Why China Is Winning the 5G War”, https://nationalinterest.org/feature/why-china-winning-5g-war-43347)

There is little doubt today that American superiority in the next generation of mobile communications, commonly called 5G, is a matter of extraordinary national concern. There is also little doubt that China is a strong competitor, already having outspent the United States by [$24 billion](https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf#page=3) and planning [$411 billion](https://www.scmp.com/tech/china-tech/article/2098948/china-plans-28-trillion-yuan-capital-expenditure-create-worlds) in 5G investment over the next decade. The Chinese government has also laid out multiple national plans for establishing the country as a leader in mobile technology, and the Chinese firm Huawei is poised to be the [top smartphone manufacturer](https://www.cnbc.com/2018/11/16/huawei-aims-to-overtake-samsung-as-no-1-smartphone-player-by-2020.html) by 2020.

And what are United States companies doing about this? Bickering over patents.

For years, the leading American supplier of advanced mobile communications chips has been the San Diego-based Qualcomm. The company has been an innovator of mobile technology, but it has also been a remarkable innovator of convoluted legal strategies. As an ongoing Federal Trade Commission [lawsuit alleges](https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-qualcomm-monopolizing-key-semiconductor-device-used), Qualcomm has used its dominant position as a chip supplier and its extensive patent holdings to weave an intricate web of patent licensing across the mobile industry. The effect of that complex licensing scheme, the FTC claims, has been to force competitor chipmakers out of the market and to extract concessions and high patent royalties from smartphone and mobile-device makers.

Qualcomm today faces only one major U.S. competitor—Intel, whose chips Apple recently [started using](https://www.cultofmac.com/484250/intel-reaping-rewards-apples-scrap-qualcomm/) instead of Qualcomm’s. Not surprisingly, Qualcomm has leveraged its patents to force a retaliatory investigation against Apple, the effect of which could be, as an administrative judge [recently determined](http://www.fosspatents.com/2018/10/itc-judge-didnt-buy-testimony-for-which.html), to boot Intel out of the mobile-chip market and leave Qualcomm as a monopoly.

It is hard to imagine that this infighting among Apple, Intel and Qualcomm is getting the United States very far in 5G, and it is harder to imagine that Qualcomm’s desired outcome would do so, either. The best path, instead, is the obvious one: allowing competition and expanding the number of firms working on 5G.

Competition encourages companies to out-innovate each other in order to grab market share. Of particular importance to 5G, competition leads to [better cybersecurity](https://morningconsult.com/opinions/in-the-race-to-5g-monopoly-considered-harmful/) in products, making them less vulnerable to hacking or misuse.

Competition is especially crucial when it comes to the technical standards that define how 5G works. These standards are the work of 3GPP, an international consortium of technology companies in the field. Chinese players such as Huawei and ZTE are major participants in 3GPP. Ensuring that 3GPP’s standards reflect American values requires having as many American companies at the negotiating table as possible—which is harder to achieve when those companies are trying to sue each other out of business.

Certainly patents themselves, as rewards for new inventions, are a driver of innovation in areas such as 5G. The problem, though, is not the existence of a patent system but the ever-expanding power of the patent laws, which encourage companies to pour dollars into complex patent licensing and assertion schemes—as companies like Qualcomm have done—rather than to perform the hard work of building new technologies. When innovation in patent strategy is more profitable than actual innovation, we lose the race to 5G and other technologies.

But don’t take my word for it. [Multiple members of Congress](https://www.patentprogress.org/2019/01/11/congress-weighs-in-on-qualcomm-and-apple-at-the-itc/), from both sides of the aisle, have denounced the use of patents to kick companies like Intel out of 5G development, predicting that such actions would “dampen the quality, innovation, competitive pricing, and in this case the preservation of a strong U.S. presence in the development of 5G and thus the national security of the United States.”

Or look to what China itself is doing. The Chinese government is handing out rewards left and right to encourage technology research and development. Indeed, it grants subsidies and financial benefits (ranging from the [ordinary](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2818503) to the [imperfect](https://funginstitute.berkeley.edu/wp-content/uploads/2013/12/patent_subsidy_Zhen.pdf) to the [bizarre](https://www.scmp.com/news/china/article/1681850/how-get-out-jail-early-china-buy-inventors-idea-and-patent-it)) to encourage its citizens to file for patents. But while China specifically encourages filing for patents, it does little to encourage using them: Patent infringement awards in court are peanuts—often only [five figures](https://scholarship.law.berkeley.edu/btlj/vol33/iss2/2/)—and most Chinese patent owners drop their patents [within five years](https://www.bloomberg.com/news/articles/2018-09-26/china-claims-more-patents-than-any-country-most-are-worthless) of getting them. The message in China is clear: You will be rewarded for innovating, but not for quibbling over patents.

The United States should take the same tack if it wants to match China in 5G. Ever-stronger patent rights encourage counterproductive disputes that are a drag on industry, a drag on research and development, and ultimately a drag on domestic competitiveness on the global stage. If America wants to lead in 5G, then it must clear the path for strong competition among leading American technology companies.

#### Chinese tech leadership upends deterrence---nuclear war.

Kroenig 18, Deputy Director for Strategy, Scowcroft Center for Strategy and Security Associate Professor of Government and Foreign Service, Georgetown University (Matthew, Nov 12, 2018, “Will disruptive technology cause nuclear war?” *BAS*, <https://thebulletin.org/2018/11/will-disruptive-technology-cause-nuclear-war>)

Rather, we should think more broadly about how new technology might affect global politics, and, for this, it is helpful to turn to scholarly international relations theory. The dominant theory of the causes of war in the academy is the “bargaining model of war.” This theory identifies rapid shifts in the balance of power as a primary cause of conflict.

International politics often presents states with conflicts that they can settle through peaceful bargaining, but when bargaining breaks down, war results. Shifts in the balance of power are problematic because they undermine effective bargaining. After all, why agree to a deal today if your bargaining position will be stronger tomorrow? And, a clear understanding of the military balance of power can contribute to peace. (Why start a war you are likely to lose?) But shifts in the balance of power muddy understandings of which states have the advantage.

You may see where this is going. New technologies threaten to create potentially destabilizing shifts in the balance of power.

For decades, stability in Europe and Asia has been supported by US military power. In recent years, however, the balance of power in Asia has begun to shift, as China has increased its military capabilities. Already, Beijing has become more assertive in the region, claiming contested territory in the South China Sea. And the results of Russia’s military modernization have been on full display in its ongoing intervention in Ukraine.

Moreover, China may have the lead over the United States in emerging technologies that could be decisive for the future of military acquisitions and warfare, including 3D printing, hypersonic missiles, quantum computing, 5G wireless connectivity, and artificial intelligence (AI). And Russian President Vladimir Putin is building new unmanned vehicles while ominously declaring, “Whoever leads in AI will rule the world.”

If China or Russia are able to incorporate new technologies into their militaries before the United States, then this could lead to the kind of rapid shift in the balance of power that often causes war. If Beijing believes emerging technologies provide it with a newfound, local military advantage over the United States, for example, it may be more willing than previously to initiate conflict over Taiwan. And if Putin thinks new tech has strengthened his hand, he may be more tempted to launch a Ukraine-style invasion of a NATO member.

Either scenario could bring these nuclear powers into direct conflict with the United States, and once nuclear armed states are at war, there is an inherent risk of nuclear conflict through limited nuclear war strategies, nuclear brinkmanship, or simple accident or inadvertent escalation.

This framing of the problem leads to a different set of policy implications. The concern is not simply technologies that threaten to undermine nuclear second-strike capabilities directly, but, rather, any technologies that can result in a meaningful shift in the broader balance of power. And the solution is not to preserve second-strike capabilities, but to preserve prevailing power balances more broadly.

When it comes to new technology, this means that the United States should seek to maintain an innovation edge. Washington should also work with other states, including its nuclear-armed rivals, to develop a new set of arms control and nonproliferation agreements and export controls to deny these newer and potentially destabilizing technologies to potentially hostile states.

These are no easy tasks, but the consequences of Washington losing the race for technological superiority to its autocratic challengers just might mean nuclear Armageddon.

#### Emergence of smart cities depends on IoT applications of 5G interoperability standards---absent FRAND, excessive royalties will undermine sustainable development.

Schwartz 18, \*Matt Schwartz, Privacy Fellowship Coordinator at ACT, App Association; (March 2nd, 2018, “It’s Smart to be FRANDly: How the FRAND Commitment Will Determine the Future of Smart Cities”, https://actonline.org/2018/03/02/its-smart-to-be-frandly-how-the-frand-commitment-will-determine-the-future-of-smart-cities/)

In December, we [outlined](https://actonline.org/2017/12/18/smart-cities-connecting-your-community-through-technology/%5d) the emergence of Smart Cities – cities that harness technological innovations like internet of things (IoT) devices and data analytics to improve essential infrastructure in growing urban centers. The technological foundation of Smart Cities aims to improve public safety, better allocate resources, and meet the needs of citizens more quickly.

A central element to Smart Cities is the comprehensive network of sensors and devices implemented within buildings, roads, traffic signs, and parking meters that allows them to interact with public, and potentially private-owned, infrastructure. These sensors will “speak” to one another, communicating information about energy usage, traffic density, or other elements of city management that have traditionally either been analyzed separately or not tracked at all. The potential of Smart Cities allows data to flow from previously disconnected branches of the city and be processed in real-time, unlocking previously unknown insights.

The powerful interoperability of Smart Cities will rely heavily on standardized technologies developed in organizations like the IEEE, which is responsible for standardizing the wi-fi technology we use every day. Standardized technologies often include standard-essential patents (SEPs), which, like their name suggests, are patents declared essential to an industry standard by a standards-setting organization. In simple terms, one cannot implement the standardized technology without using the patent.

Like regular patents, the users of SEPs must pay royalties or licensing fees to the patent owner before they may use it. For example, if a manufacturing company wants to make an IoT device interoperable with a 5G network, the manufacturer must pay a licensing fee to the owner of the SEP that is essential to the 5G standard. SEPs play a vital role in the new innovations we enjoy and have come to expect, and because of the value of these patents, SEP holders have the ability to demand high license fees from those who wish to implement the standard. To offset this competition issue, many SEP holders voluntarily agree to license their SEPs to any willing licensee under fair, reasonable, and non-discriminatory (FRAND) terms.

While wi-fi and LTE are standards that will be vital to Smart City deployment, countless new standardized technologies are being developed that will be integral to any fully-operational Smart City. With reasonable access to SEPs, assured by the FRAND commitment, innovators can enjoy the legal and business certainty they need to compete. While the meaning of the FRAND commitment continues to be refined – as evidenced by the development of SEP best practices recently launched by the App Association in Europe – its foundations are well-established.

But what happens when SEP holders do not abide by the FRAND licensing commitment, or simply refuse to license at all? Sadly, small and medium-sized companies would be forced to accept untenable licensing terms, but more realistically, they would be priced out of using the standard altogether. As a result, it would impose a barrier to innovation that would result in fewer products offered to consumers or cities eager to implement IoT technologies. For example, many hope the rise of autonomous vehicles will be seamlessly integrated into the Smart City network. But how beneficial would it be if only some autonomous vehicle brands are able to license the technology needed to communicate with traffic lights, simply because of the market power of a chipmaker? The FRAND commitment is an important backstop to that unfortunate possibility.

It is vital for SEP holders to honor FRAND licensing terms, if not for small and medium-sized innovators, then for the sustainability of future Smart Cities. FRAND creates a platform for innovation, providing a floor on which companies can stand, innovate, and compete. If the foundation of the FRAND commitment is reneged, American innovators pay a steep price – not only do they lose a key component of product development and market entry, but they are also left with years of expensive negotiations and litigation if they choose to challenge the licensing practice. What’s more, the confidence developed in the open standards development system is shaken, and Smart Cities have fewer choices in IoT solutions for their future.

To achieve the promise of Smart Cities, a balanced standards ecosystem is essential. We must allow small and medium-sized developers to leverage industry standards for innovation and prevent cost-prohibitive royalty structures and negotiating practices that are detrimental to competition, while also ensuring that SEP owners can protect their intellectual property and be fairly compensated for its use. The FRAND commitment continues to be the best framework to achieve this balance, and adherence to its principles will determine the future and success of Smart Cities.

#### Climate change is anthropogenic and causes extinction---5G-enabled smart cities are critical for mitigation and adaptation.

Huseien 21, \*Ghasan Fahim Huseien is a research fellow at Department of Building, School of Design and Environment, National University of Singapore, Singapore; Dr. Kwok Wei Shah is presently an assistant professor and deputy program director with the Department of Building, School of Design and Environment, National University of Singapore, Singapore; (August 23rd, 2021, “Potential Applications of 5G Network Technology for Climate Change Control: A Scoping Review of Singapore”, https://www.mdpi.com/2071-1050/13/17/9720)

Currently, the entire planet is at risk due to continual climate change [1–3]. The recorded increase in average temperature across the world in the past hundred years, and the associated changes attributed to this, are known as global warming. Many scientists are convinced by the published evidence that this change is anthropogenic and resulted from the elevated emission levels of global greenhouse gases (GHGs) [4,5]. Gases such as water vapor, carbon dioxide, methane, nitrous oxide, and ozone are responsible for the absorption and emission of thermal radiation. These changes in the relative quantities of the GHGs induce a proportional change in the amount of preserved solar energy. Presently, the accepted indicator for global warming is the sustained rise in the mean temperature worldwide. This definition is designed to account for the fact that there may be some localized exceptions to this rise. For example, there may be cooling experienced in a region while the global temperature may increase altogether, hence the need for average temperature. A key concern with the GHGs trapping of more heat in the atmosphere is that it affects both climate and short scale weather patterns. Consequently, it results in greater numbers of adverse weather events such as storms, heat waves, cold snaps, droughts, and fires [6]. Climate-related risks to health, livelihoods, food security, water supply, human safety, and economic growth are projected to increase with global warming of 1.5 ◦C [7] and further increase further at 2 ◦C, as shown in Figure 1. In addition, the risks to global aggregated economic growth due to the climate change impacts are projected to be lower at 1.5 ◦C than at 2 ◦C by the end of this century.

Carbon dioxide has the most substantial effect on global warming [8]. Although it was once assumed to have an ~100 year lifespan in the atmosphere, careful studies revealed that the situation is far worse, with three-quarters of the gas expected to remain for a time in the region of up to ~1000 years, with the remainder lasting for an indefinite period of time [9]. It was indicated that the present impacts of humanity on the atmosphere can certainly cause a long term problem [10]. Carbon dioxide is released when oil, coal, and other fossil fuels are burnt for the energy we use to power our homes, cars, and smartphones. By lessening its usage, we can curb our own contribution to climate change while saving money. The first challenge is eliminating the burning of coal, oil, and, eventually, natural gas. Oil is the lubricant of the global economy as it is hidden inside such ubiquitous items as plastic and corn, fundamental to the transportation of both consumers and goods. Coal is the substrate, supplying roughly half of the electricity worldwide, a percentage that is likely to grow according to the International Energy Agency (IEA). In fact, buildings contribute up to 43% of all the greenhouse gas emissions worldwide [11], even though investing in thicker insulation and other cost-effective as well as temperature-regulating strategies can save money in the long run. Investment in new infrastructures, or radical upgradation of the existing highways and transmission lines, may help to reduce greenhouse gas emissions, yielding economic growth in the developing countries.

Nations across the globe have kept very high targets to reducing their GHG discharges [12,13]. In order to meet these goals, considerable reductions in city energy usage is required. At a global scale, urban communities represent over half (55%) of the population, which is predicted to reach 68% by the middle of this century [14]. Urban areas claim ownership of the highest levels of energy use, gas emission, and also the largest local economy. As such, it is crucial for urban areas to reduce their consumption and utilize renewable sources wherever available to reduce their gas discharge levels. Smart cities often utilize digital sensors to measure and transmit data about the levels of GHGs in the city at that moment, as a means of tackling them [15]. The efficacy of such a system is thus reliant on the network used to collate and analyze the data collected as an extant network. The mobile telecommunications networks offer a convenient solution to this desire, as their pre-existence has the clear benefit of reducing costs compared to the design and implementation of a novel system. It is recognized that smart cities will certainly act as the key players meeting these ambitious targets [16,17]. In this study, we focused primarily on the potential applications of 5G network technology to control climate change in Singapore. In addition, a clear overview of the sustainability benefits of introducing 5G technology compatible smart cities, buildings, and farms in all aspects of urbanization is provided. Herein, the main purpose is to tackle the negative outcomes associated with anthropogenic climate change, with a particular focus on the contributions that are best made by the telecoms network operators.

Climate change is one of the most challenging problems that humanity has ever faced. Presently, hundreds of millions of lives, innumerable species, entire ecosystems, health, economy, and the future habitability of this planet are at risk. Fortunately, climate change is solvable, we just need to wisely exploit the existing technologies and sciences. Climate change mitigation is a pressing international need in which many management actions are required. The development of 5G technology has been largely driven by smart mobile devices and advanced communication technologies. It may thus serve as a technical enabler for a whole new range of business opportunities, energy, and facilities management, together with industrial applications. Moreover, it may enable different devices to work together seamlessly. Definitely, the 5G cellular network technology is expected to revolutionize the global industries with profound effects on the savings of energy, waste generation and recycling, and water resources management, thus reducing the climate change impacts.

### 1AC — Cybersecurity

#### Advantage 2 is Cybersecurity —

#### Aggressive patent strategies create structural flaws in 5G standardization that imperils domestic cybersecurity---market competition reduces the incidence of vulnerability and severity of attacks.

Duan 20, \*Charles Duan is a senior fellow and associate director of tech & innovation policy at the R Street Institute, where he focuses his research on intellectual property issues; (2020, “OF MONOPOLIES AND MONOCULTURES: THE INTERSECTION OF PATENTS AND NATIONAL SECURITY”, Santa Clara High Technology Law Journal, 36(4), 369-405. Retrieved from <https://www2.lib.ku.edu/login?url=https://www.proquest.com/scholarly-journals/monopolies-monocultures-intersection-patents/docview/2442966690/se-2?accountid=14556>)

III. COMPETITION AND CYBERSECURITY

In addition to the historical review done so far, another approach to understanding the relationship among patents, competition, and national security is to consider the role of cybersecurity. There is little doubt that computer system vulnerabilities that enable hacking and spread of computer exploits are a threat to the nation’s defenses, so better cybersecurity is a key part of national security strategy.155

Strong competition can thus complement national security by enhancing domestic cybersecurity, and patent assertion that unduly weakens competition detracts from cybersecurity.156 Competition promotes better cybersecurity in at least two ways. First, multiple studies show that competition encourages firms to improve their products on multiple vectors including cybersecurity. Second, competition avoids a situation that security experts call a “monoculture,” which increases vulnerability to severe cyberattacks. As former Secretary of Homeland Security Michael Chertoff wrote recently, “We need competition and multiple providers, not a potentially vulnerable technological monoculture,” to guarantee national security.157 Thus, cybersecurity provides a useful lens for understanding how unfettered patent assertion and licensing can detract from national security.

A. Cybersecurity as Competitive Value-Add

Competition enhances national security by reducing the incidence of technical vulnerabilities. That effect is especially important for security sensitive systems such as mobile telecommunications.

Intuitively, a causal chain from competition to cybersecurity makes logical sense. Computer security is a value-added benefit to consumers, so firms in competitive markets are likely to use security to gain an edge over their competitors.158 In monopolized markets, though, there may be less external impetus to test products for flaws, and the monopolist may choose to focus less on security and more on new product features or increased product quality.

Economic research confirms these hypotheses about competition leading to better cybersecurity. A 2009 empirical study of web browsers considered the impact of market concentration on the amount of time that vendors took to fix security vulnerabilities as they were discovered.159 The study found that the presence of more competitors correlated with faster cybersecurity response—a reduction of 8–10 days in response time per additional market rival.160 Similarly, business researchers in 2005 modeled incentives for firms to engage in sharing of cybersecurity information, and concluded that the “inclination to share information and invest in security technologies increases as the degree of competitiveness in an industry increases.”161 Another study found that, where two software firms are in competition, at least one will be willing to take on some degree of risk and responsibility for cybersecurity, whereas a monopoly software firm will consistently fail to accept such responsibility.162 To be sure, an unpublished study from 2017 found that some market concentration can make firms more responsive to cybersecurity issues, but only to a point: “being in a dominant position reduces the positive effect of having less competitors on the responsiveness of the vendor,” and indeed the “more dominant the firm is, the less rapid it is in releasing security patches.”163 This research confirms that competition is more conducive to cybersecurity.

It is not hard to see how this applies to emerging communication technologies markets. In the absence of competition, the above research suggests that device manufacturers, chip makers, and software developers will lack incentives to respond to vulnerabilities, to share information about cybersecurity practices and issues, and to take responsibility for security matters. Mobile phone chips have had their share of cybersecurity failures already.164 The best way to flush out ongoing and future cybersecurity issues is to maintain competitive pressure at all levels of the supply chain.

B. Vulnerabilities of “Monocultures”

A second reason why monopoly undermines cybersecurity is that monopoly leads to a “monoculture” of single-vendor products, opening the door to massive systemic failure in the case of a cyberattack. Computer researchers developed the theory of software monocultures in the early 2000s, in response to the regular phenomenon of computer viruses and other attacks spreading rapidly by exploiting flaws in the dominant operating system at the time, Microsoft Windows.165 Where a computer system such as Windows has a commanding share of users, a virus that exploits a flaw in that system can quickly spread to infect a whole interconnected ecosystem. An operating system monopoly thus enables fast and easy spread of cyberattacks, and better cybersecurity would be achieved through greater diversity in online systems.166 As one research group posited, “a network architecture that supports a collection of heterogeneous network elements for the same functional capability offers a greater possibility of surviving security attacks as compared to homogeneous networks.”167

There has been considerable study of the theory that computer monocultures are naturally more vulnerable to attacks.168 In one study, computer science researchers reviewed a catalog of 6,340 software vulnerabilities recorded in 2007, to compare whether comparable software would share the same flaws.169 Of the 2,627 vulnerabilities applicable to application software (as opposed to operating systems, web scripts, and other software components), only 29 (1.1%) applied to substitute products from different vendors but providing the same functionality.170 By contrast, different versions of a single software product were found to share vulnerabilities 84.7% of the time.171 Thus, software monocultures share exploitable flaws even when there is some variation in versions across the monoculture; by contrast, diversity in software is almost guaranteed to prevent a single flaw from affecting all users.

In the case of 5G and wireless mobile communications, a monoculture is an especially concerning possibility. To the extent that systems such as smart city sensors or communication networks are widely deployed in a monoculture fashion, a widespread attack could have devastating consequences, potentially blacking out a region and affecting essential services such as 911.172 A monoculture that is vulnerable to so-called “rootkits” or “backdoors”—maliciously installed software that enable bad actors to commandeer systems—could also enable mass surveillance or spying by private hackers or foreign governments.173 The presence of systems from multiple vendors would mitigate these possibilities.

The monoculture theory is not without critics, but a review of those criticisms shows them to be inapplicable to contemporary communication technologies. Some critics suggest that software diversity imposes unwarranted costs on firms who must forego economies of scale and devise seemingly duplicative yet different setups of computer systems.174 But those concerns largely focus on the situation where a single firm produces and manages heterogeneous systems, concerns that are avoided where heterogeneity arises naturally through competition between two unrelated firms. Critics also argue that technological measures can create “artificial diversity” through automated randomization of software code, so software engineers can purportedly solve monoculture issues and device users need not worry about the issue.175 But even these critics acknowledge that artificial diversity techniques are often insufficient because they must make assumptions about what aspects of the technology are most vulnerable to attack, and they concede that artificial diversity cannot stop attacks involving operation of legitimate software functions in undesirable ways (sending spam emails or deleting document files, for example).176

It is widely recognized that a monoculture is unavoidable in at least one respect: Most connected devices will need to conform to technical standards.177 5G, for example, is a technical standard developed by a private industry consortium called 3GPP.178 A flaw in any such standard would render all mobile devices implementing the standard vulnerable to an identical attack.179 Avoiding these sorts of systemic flaws in standards requires rigorous development, analysis, and testing of the standard in the development process, which in turn requires ensuring that as many firms as possible, especially firms that share basic American values, are involved in the development of those standards.180 Thus, the necessary standardization of information and communication technologies is perhaps the most important reason why a competitive communication technology market is essential to cybersecurity and national security.

#### Insecure technical standards cause inevitable systemic grid collapse---extinction.

DeNardis 21, \*Dr. Laura DeNardis, PhD in Science and Technology Studies from Virginia Tech, Dean of the School of Communication at American University, and Gordon M. Goldstein, Adjunct Senior Fellow at the Council on Foreign Relations, (March 1st, 2021, “The Real Lesson of the Texas Power Debacle”, Lawfare, 3/1/2021, https://www.lawfareblog.com/real-lesson-texas-power-debacle)

The infrastructure was essential, ubiquitous and providing basic functionality for everything in daily life from water to heat and transportation. And in an instant it was gone, plunging tens of thousands of residents into a life-threatening crisis. This is, of course, the narrative of the recent debacle in Texas, where a winter storm overwhelmed the state’s electrical grid and brought the state to a near-total blackout. But it should also be interpreted as a preemptive warning of what Americans will face from the next generation of the internet and the new realm of cybersecurity risk it will dramatically amplify.

Both forms of infrastructure—a state-run electrical grid and the 5G and “internet of things” future to which we are rapidly hurtling—share three attributes. First, their construction reflects a lack of imagination about the danger that can quickly coalesce when seemingly remote threat scenarios become real. Second, compounding a lack of analytic imagination is an absence of preparedness. Third, for both the Texas electrical grid and the emerging internet, public policy protections are either meager or completely absent.

In planning for the resilience of its electrical grid, public officials in Texas discounted the potentially devastating disruption that could occur from unpredictable events—whether related to climate change or just a once-a-century anomaly. They also eschewed precautions other states take seriously by allowing for the interconnection of electrical grid supply chains across their borders, ostensibly because of their ideological rejection of federal regulatory oversight governing such arrangements.

As the United States builds out a new national 5G cyber-physical communications network through private service providers, Americans similarly discount the risks—myriad in their diversity and severity—that are orders of magnitude more significant than what Texas confronted recently. More physical things than people are already connected. The super empowered internet of tomorrow, known among some in the field as the “internet of everything,” will exceed by tens of billions of devices the number of connections between individuals simply communicating via social media or digital screens.

This confronts policymakers with an imminent threat: A cyber outage is no longer about losing digital communications but about losing basic societal functioning and even human life. The failure of imagination is to think of the SolarWinds attack on U.S. federal agencies and tech companies as a worst-case scenario. The failure of imagination is to think of cybersecurity through a content-centric lens rather than as possible attacks on the material world. The emergence of internet-connected cardiac devices, digitally dependent cars, and internet-connected agriculture systems portend the stakes of a cyberattack to health care, economic and social functioning, and food security.

The United States should be prepared for, and certainly not be caught by surprise by, such cyberattacks. Yet, the internet of everything is notoriously insecure. Internet-connected physical objects are not necessarily upgradeable. Nor do they come with adequate default security and encryption. The 5G infrastructure that helps connect digital objects has been at the center of debates over Chinese espionage. Industrial cyber-physical systems are based on technical standards that have not been collaboratively vetted for security and interoperability. One of the most infamous cyberattacks—the so-called Mirai botnet that took down major media sites and corporations—hijacked these insecure objects in homes to carry out the assault. The United States is not yet prepared.

Finally, in the race to conceive and deploy effective public policy responses, the U.S. government as a whole is hardly more anticipatory or synthesized in its response to potential calamity than the state of Texas. The focus of U.S. cyber policy remains on information policy issues such as disinformation, manipulation and violent speech rather than securing the digital world that now powers our material day-to-day lives. The Biden administration confronts an enormous challenge in crafting a comprehensive strategy to the cybersecurity risks foreshadowed by the ruinous experience in Texas and its management of vital infrastructure. While the digital world has leapt from two-dimensional to three-dimensional space, cyber policy has not at all jumped from 2D to 3D.

This failure of imagination, preparedness and policy protection must not be America’s cyber future; the stakes are far too high and the costs are far too great. The Texas disaster is a potent illustration of what has always been true: Our digital society and economy are extremely vulnerable and grow more porous and subject to penetration day by day. As digital sensors and cyber control systems become further embedded in physical infrastructure like energy systems, agriculture and transportation, there is no longer a separation between security of the “real” world and security of the online world. They are entangled and increasingly enmeshed—and policy has yet to catch up to either envisioning or mitigating the looming threats the U.S. confronts.

If the energy grid cannot weather a winter storm, how can it be expected to withstand a major cyberattack? What other vital forms of national infrastructure—ranging from water, bridges, highways and roads, and ultimately our day-to-day financial system—are comparably at risk? As Texas dramatizes, it is neither hyperbolic nor exaggerated to assert that our survival could now depend on securing the inevitable cyber-physical future that is accelerating with stunning rapidity.

#### Actors have the means and motivations to strike critical infrastructure.

Wintch 21, \*Timothy M. Wintch, an active-duty Major in the United States Air Force. He is currently a graduate student at the Oettinger School of Science & Technology Intelligence, National Intelligence University, in Bethesda, Maryland. Mr. Wintch has over 11 years of experience in command-and-control operations as an Air Battle Manager. He holds a Bachelor of Arts in Politics from the University of California, Santa Cruz, and a Master of Arts in Military Studies from American Military University. (April 20th, 2021, “PERSPECTIVE: Cyber and Physical Threats to the U.S. Power Grid and Keeping the Lights on”, https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/)

Among critical infrastructure sectors in the U.S., energy is perhaps the most crucial of the 16 sectors defined by the Department of Homeland Security. This sector is so vital because it provides the energy necessary to run every other critical infrastructure sector. However, the U.S. power grid, the backbone of the energy sector, is built upon an aging skeleton that is becoming increasingly vulnerable every day. Whether from terrorists or nation-states like Russia and China, the power grid is susceptible to not just physical attacks, but also to cyber intrusion as well. However, much of this threat can be mitigated if the U.S. takes the appropriate steps to safeguard the power grid and avoid a potential catastrophe in the future.

Since Sept. 11, 2001, terrorism on U.S. soil has been at the forefront of American consciousness. Critical infrastructure provides an appealing target because of the disproportionally large impact even a small attack can have on the sectors. In particular, the power grid represents a particularly lucrative target, both in terms of the ease of access and the large impact it can make. The National Research Council stated that the U.S. power grid is “vulnerable to intelligent multi-site attacks by knowledgeable attackers intent on causing maximum physical damage to key components on a wide geographical scale.”[[1]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn1) Additionally, the physical security of transmission and distribution systems is difficult due to the dispersed nature of these key components, which in turn is advantageous to attackers as it reduces the likelihood of their capture.[[2]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn2) From 2002-2012, approximately 2,500 physical attacks occurred against transmission lines and towers worldwide and approximately 500 attacks against transformer substations.[[3]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn3) Terrorists have the motivation to attack the U.S. power grid but the very nature of the grid makes it highly vulnerable. The power grid is not only at risk from physical attacks, but also nation-state cyberattacks.

One nation that has shown both the capability and intent to use attacks against critical energy infrastructure is Russia, as demonstrated in their 2015 annexation of Crimea from Ukraine. A Russian cyber threat group known as Sandworm, which used its BlackEnergy malware, attacked Ukrainian computer systems that provide remote control of the Ukraine power grid.[[4]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn4) This attack, and another in 2016, each left the capital Kiev without power, prompting cyber experts to raise concern about the same malware already existing in NATO and the U.S. power grids.[[5]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn5) In any conflict between Russia and NATO, not only would similar cyberattacks pose a threat, but so would potential physical attacks severing fuel oil and natural gas lines to Western Europe. Russia has both the capability and intent to attack critical infrastructure, particularly power grids, during future conflicts in their “hybrid warfare” approach.

Another nation that has the capability to attack critical energy infrastructure is China, representing a threat to not just the U.S. energy infrastructure but also that of our allies whose support would be vital in a major conflict. A recent NATO report highlighted this threat from China’s Belt and Road Initiative, stating that “[China’s] foreign direct investment in strategic sectors [such as energy generation and distribution] …raises questions about whether access and control over such infrastructure can be maintained, particularly in crisis when it would be required to support the military.”[[6]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn6) Like Russia, China has been active with cyber intrusions in U.S. energy infrastructure. The Mission Support Center at Idaho National Laboratory characterized these as attacks as “multiple intrusions into US ICS/SCADA [Industrial Control Systems/Supervisory Control and Data Acquisition] and smart grid tools [that] may be aimed more at intellectual property theft and gathering intelligence to bolster their own infrastructure, but it is likely that they are also using these intrusions to develop capabilities to attack the [bulk electric system], as well.”[[7]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn7) China, therefore, has both the capability and intent to conduct cyber intrusions and attacks for myriad reasons.

Another arm of this threat is the reliance the U.S. energy industry has on imports from China, especially transformers. In early 2020, federal officials seized a transformer in the port of Houston that had been imported by the Jiangsu Huapeng Transformer Company before sending it to Sandia National Laboratory in Albuquerque. Sandia is contracted by the U.S. Department of Energy for mitigating national security threats.[[8]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn8) The Wall Street Journal reported that “Mike Howard, chief executive of the Electric Power Research Institute, a utility-funded technical organization, said that the diversion of a huge, expensive transformer is so unusual – in his experience, unprecedented – that it suggests officials had significant security concerns.”[[9]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn9) Previously destined for the Washington Area Power Administration’s Ault, Colo., substation, the transformer is believed to have been seized due to “backdoor” exploitable hardware emplaced by the Chinese prior to shipment.[[10]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn10) Shortly after these events, President Trump issued Executive Order 13920, “[Securing the United States Bulk-Power System](https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/),” essentially limiting the import of Chinese-built critical energy infrastructure components due to concerns about cybersecurity.[[11]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn11) Interestingly, Jiangsu Huapeng “boasted that it supported 10 percent of New York City’s electricity load.”[[12]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn12)

Franklin Kramer, the former Assistant Secretary of Defense for International Security Affairs, testified before a U.S. House of Representatives Energy and Commerce subcommittee during an energy and power hearing in 2011 and said that a “highly-coordinated and structured cyber, physical, or blended attack on the bulk power system, however, could result in long-term (irreparable) damage to key system components in multiple simultaneous or near-simultaneous strikes.” He added that “an outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods.”[[13]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn13) Even the inclusion of features such as smart grids to the overall grid structure poses new vulnerabilities through their connectivity. Kramer stated that “such connectivity means that the distribution system could be a key vector for a national security attack on the grid.”[[14]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn14)

#### Those attacks cause accidental nuclear escalation.

Klare 19, \*Michael T. Klare is a professor emeritus of peace and world security studies at Hampshire College and senior visiting fellow at the Arms Control Association; (November 19th, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation”, https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation)

Yet another pathway to escalation could arise from a cascading series of cyberstrikes and counterstrikes against vital national infrastructure rather than on military targets. All major powers, along with Iran and North Korea, have developed and deployed cyberweapons designed to disrupt and destroy major elements of an adversary’s key economic systems, such as power grids, financial systems, and transportation networks. As noted, Russia has infiltrated the U.S. electrical grid, and it is widely believed that the United States has done the same in Russia.[12](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote12) The Pentagon has also devised a plan known as “Nitro Zeus,” intended to immobilize the entire Iranian economy and so force it to capitulate to U.S. demands or, if that approach failed, to pave the way for a crippling air and missile attack.[13](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote12)

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread chaos and harm and eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, such attacks “could lead to major conflict and possibly nuclear war.”[14](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote14)

These are by no means the only pathways to escalation resulting from the offensive use of cyberweapons. Others include efforts by third parties, such as proxy states or terrorist organizations, to provoke a global nuclear crisis by causing early-warning systems to generate false readings (“spoofing”) of missile launches. Yet, they do provide a clear indication of the severity of the threat. As states’ reliance on cyberspace grows and cyberweapons become more powerful, the dangers of unintended or accidental escalation can only grow more severe.

#### Cyber-compromised NC3 causes nuclear war.

Klare 19, \*Michael T. Klare is a professor emeritus of peace and world security studies at Hampshire College and senior visiting fellow at the Arms Control Association; (November 19th, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation”, <https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation>)

The Nuclear-Cyber Connection

These links exist because the NC3 systems of the United States and other nuclear-armed states are heavily dependent on computers and other digital processors for virtually every aspect of their operation and because those systems are highly vulnerable to cyberattack. Every nuclear force is composed, most basically, of weapons, early-warning radars, launch facilities, and the top officials, usually presidents or prime ministers, empowered to initiate a nuclear exchange. Connecting them all, however, is an extended network of communications and data-processing systems, all reliant on cyberspace. Warning systems, ground- and space-based, must constantly watch for and analyze possible enemy missile launches. Data on actual threats must rapidly be communicated to decision-makers, who must then weigh possible responses and communicate chosen outcomes to launch facilities, which in turn must provide attack vectors to delivery systems. All of this involves operations in cyberspace, and it is in this domain that great power rivals seek vulnerabilities to exploit in a constant struggle for advantage.

The use of cyberspace to gain an advantage over adversaries takes many forms and is not always aimed at nuclear systems. China has been accused of engaging in widespread cyberespionage to steal technical secrets from U.S. firms for economic and military advantages. Russia has been accused, most extensively in the Robert Mueller report, of exploiting cyberspace to interfere in the 2016 U.S. presidential election. Nonstate actors, including terrorist groups such as al Qaeda and the Islamic State group, have used the internet for recruiting combatants and spreading fear. Criminal groups, including some thought to be allied with state actors, such as North Korea, have used cyberspace to extort money from banks, municipalities, and individuals.[4](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote04) Attacks such as these occupy most of the time and attention of civilian and military cybersecurity organizations that attempt to thwart such attacks. Yet for those who worry about strategic stability and the risks of nuclear escalation, it is the threat of cyberattacks on NC3 systems that provokes the greatest concern.

This concern stems from the fact that, despite the immense effort devoted to protecting NC3 systems from cyberattack, no enterprise that relies so extensively on computers and cyberspace can be made 100 percent invulnerable to attack. This is so because such systems employ many devices and operating systems of various origins and vintages, most incorporating numerous software updates and “patches” over time, offering multiple vectors for attack. Electronic components can also be modified by hostile actors during production, transit, or insertion; and the whole system itself is dependent to a considerable degree on the electrical grid, which itself is vulnerable to cyberattack and is far less protected. Experienced “cyberwarriors” of every major power have been working for years to probe for weaknesses in these systems and in many cases have devised cyberweapons, typically, malicious software (malware) and computer viruses, to exploit those weaknesses for military advantage.[5](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote05)

Although activity in cyberspace is much more difficult to detect and track than conventional military operations, enough information has become public to indicate that the major nuclear powers, notably China, Russia, and the United States, along with such secondary powers as Iran and North Korea, have established extensive cyberwarfare capabilities and engage in offensive cyberoperations on a regular basis, often aimed at critical military infrastructure. “Cyberspace is a contested environment where we are in constant contact with adversaries,” General Paul M. Nakasone, commander of the U.S. Cyber Command (Cybercom), told the Senate Armed Services Committee in February 2019. “We see near-peer competitors [China and Russia] conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage.”

Although eager to speak of adversary threats to U.S. interests, Nakasone was noticeably but not surprisingly reluctant to say much about U.S. offensive operations in cyberspace. He acknowledged, however, that Cybercom took such action to disrupt possible Russian interference in the 2018 midterm elections. “We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts,” he testified in February. According to press accounts, this included a cyberattack aimed at paralyzing the Internet Research Agency, a “troll farm” in St. Petersburg said to have been deeply involved in generating disruptive propaganda during the 2016 presidential elections.[6](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote06)

Other press investigations have disclosed two other offensive operations undertaken by the United States. One called “Olympic Games” was intended to disrupt Iran’s drive to increase its uranium-enrichment capacity by sabotaging the centrifuges used in the process by infecting them with the so-called Stuxnet virus. Another left of launch effort was intended to cause malfunctions in North Korean missile tests.[7](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote07) Although not aimed at either of the U.S. principal nuclear adversaries, those two attacks demonstrated a willingness and capacity to conduct cyberattacks on the nuclear infrastructure of other states.

Efforts by strategic rivals of the United States to infiltrate and eventually degrade U.S. nuclear infrastructure are far less documented but thought to be no less prevalent. Russia, for example, is believed to have planted malware in the U.S. electrical utility grid, possibly with the intent of cutting off the flow of electricity to critical NC3 facilities in the event of a major crisis.[8](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote08) Indeed, every major power, including the United States, is believed to have crafted cyberweapons aimed at critical NC3 components and to have implanted malware in enemy systems for potential use in some future confrontation.

Pathways to Escalation

Knowing that the NC3 systems of the major powers are constantly being probed for weaknesses and probably infested with malware designed to be activated in a crisis, what does this say about the risks of escalation from a nonkinetic battle, that is, one fought without traditional weaponry, to a kinetic one, at first using conventional weapons and then, potentially, nuclear ones? None of this can be predicted in advance, but those analysts who have studied the subject worry about the emergence of dangerous new pathways for escalation. Indeed, several such scenarios have been identified.[9](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote09)

The first and possibly most dangerous path to escalation would arise from the early use of cyberweapons in a great power crisis to ~~paralyze~~ undermine the vital command, control, and communications capabilities of an adversary, many of which serve nuclear and conventional forces. In the “fog of war” that would naturally ensue from such an encounter, the recipient of such an attack might fear more punishing follow-up kinetic attacks, possibly including the use of nuclear weapons, and, fearing the loss of its own arsenal, launch its weapons immediately. This might occur, for example, in a confrontation between NATO and Russian forces in east and central Europe or between U.S. and Chinese forces in the Asia-Pacific region.

Speaking of a possible confrontation in Europe, for example, James N. Miller Jr. and Richard Fontaine wrote that “both sides would have overwhelming incentives to go early with offensive cyber and counter-space capabilities to negate the other side’s military capabilities or advantages.” If these early attacks succeeded, “it could result in huge military and coercive advantage for the attacker.” This might induce the recipient of such attacks to back down, affording its rival a major victory at very low cost. Alternatively, however, the recipient might view the attacks on its critical command, control, and communications infrastructure as the prelude to a full-scale attack aimed at neutralizing its nuclear capabilities and choose to strike first. “It is worth considering,” Miller and Fontaine concluded, “how even a very limited attack or incident could set both sides on a slippery slope to rapid escalation.”[10](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote10)

What makes the insertion of latent malware in an adversary’s NC3 systems so dangerous is that it may not even need to be activated to increase the risk of nuclear escalation. If a nuclear-armed state comes to believe that its critical systems are infested with enemy malware, its leaders might not trust the information provided by its early-warning systems in a crisis and might misconstrue the nature of an enemy attack, leading them to overreact and possibly launch their nuclear weapons out of fear they are at risk of a preemptive strike.

“The uncertainty caused by the unique character of a cyber threat could jeopardize the credibility of the nuclear deterrent and undermine strategic stability in ways that advances in nuclear and conventional weapons do not,” Page O. Stoutland and Samantha Pitts-Kiefer wrote in 2018 paper for the Nuclear Threat Initiative. “[T]he introduction of a flaw or malicious code into nuclear weapons through the supply chain that compromises the effectiveness of those weapons could lead to a lack of confidence in the nuclear deterrent,” undermining strategic stability.[11](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote11) Without confidence in the reliability of its nuclear weapons infrastructure, a nuclear-armed state may misinterpret confusing signals from its early-warning systems and, fearing the worst, launch its own nuclear weapons rather than lose them to an enemy’s first strike. This makes the scenario proffered in the 2018 NPR report, of a nuclear response to an enemy cyberattack, that much more alarming.

### 1AC — Plan

#### Plan: The United States federal judiciary should substantially increase prohibitions on private sector conduct that is more restrictive of competition than reasonably necessary to enable creation of information technology standards.

### 1AC — Solvency

#### Solvency —

#### The plan requires SSO’s to administer reasonable action to prohibit ex post opportunism---that strengthens FRAND effectiveness while enabling SEP holders to capture appropriate royalties---which is the best competition-innovation balance.

Melamed & Shapiro 18, \*A. Douglas Melamed is Professor of the Practice of Law at Stanford Law School; \*Carl Shapiro is the Transamerica Professor of Business Strategy at the Haas School of Business at the University of California at Berkeley; (May 2018, “How Antitrust Law Can Make FRAND Commitments More Effective”, https://www-cdn.law.stanford.edu/wp-content/uploads/2018/05/How-Antitrust-Law-Can-Make-FRAND-Commitments-More-Effective.pdf)

3. Application of the Basic Legal Principles

The antitrust principle is straightforward: industry-wide collaboration through SSOs to establish procompetitive standards is permitted only if it is no more restrictive of competition than reasonably necessary to enable creation of the standards. When standard setting predictably creates technology monopolies that, if unrestrained, will enable anticompetitive ex post opportunism that would otherwise not occur, an SSO that does not take effective measures to prevent or minimize such ex post opportunism engages in conduct that is more restrictive of competition than necessary. In that case, the SSO and, in appropriate cases, its members, may well violate Section 1 of the Sherman Act.

Under this principle, SSO procedures and FRAND rules should be evaluated based on whether they lead to reasonable SEP royalties, using the competitive ex ante licensing standard discussed above, which has been adopted by the courts in patent law. Put differently, FRAND rules should be evaluated based on their ability to prevent SEP holders from obtaining more than the ex ante value of their technology from implementers.

This limitation would not prevent a SEP holder from proﬁting, perhaps greatly, from participating in the SSO and having its patented technology included in the standard. The SEP holder continues to be rewarded for its technology because the inclusion of its technology in the standard can still greatly increase the volume of licensing opportunities available to the SEP holder.

Whether a particular set of FRAND rules are sufficiently effective in preventing ex post opportunism will depend on the particular circumstances. The procedural unfolding of the case will also depend upon the circumstances. As a general matter, the case would probably be structured as an ordinary Rule of Reason case.82

First, the plaintiff would have to demonstrate harm to competition as a result of the collaboration of the SSO’s members, many of which compete with one another. In this case, the harm to competition would stem from the ability of the SEP holder to exercise monopoly power by obtaining royalties in excess of the competitive, ex ante level. The decision to include patented technologies in the standard would be the allegedly unlawful agreement. Notably, the court need not determine what a FRAND royalty is; it would suffice to determine that market power has been created or exercised, and that existing SSO rules and policies were not adequate to prevent the competitive harm. The defendant, which could be the SSO or perhaps one or more SSO members, would win at this point if the plaintiff failed to show harm to competition. If might fail if the standard faces substantial competition and the court concludes that the SEP holder therefore does not have market power or if the SSO’s rules and policies are found to be effective in preventing ex post opportunism, even if the plaintiff or even the court thinks that other rules and policies would be preferable.

Second, if the plaintiff makes the requisite showing of harm to competition, the defendant(s) would then have to show some procompetitive justiﬁcation— in this case, the beneﬁts of the standard. These two initial steps should be straightforward.

Third, if as is likely the defendant is able to show a procompetitive justiﬁcation, the plaintiff would have to show that the SSO could have used available, reasonable alternatives to realize the efficiency beneﬁts with less or none of the competitive harms. The plaintiff might identify reasonable alternatives that would have led to a different standard, based on including unpatented technology in the standard or perhaps involving fewer SEPs or fewer owners of SEPs, which would be less subject to patent holdup. More likely, the plaintiff could suggest alternative SSO rules that would not change the standard, but would reduce the likelihood or extent of ex post opportunism. For example, the plaintiff might suggest more rigorous FRAND-type rules, such as rules that set forth more precise principles on which FRAND royalties are to be determined and the circumstances under which SEP holders might seek injunctions.

Fourth, the burden would then shift to the defendant(s) to show that the beneﬁts of the standard could not have been realized if the SSO had adopted any of the proffered alternatives or that those alternatives were unrealistic.83 The plaintiff would be entitled to judgment if the court concludes that those beneﬁts could have been realized with less competitive harm if the SSO had adopted the standard with different IPR rules or policies.

Our overall sense, based on experience and the empirical literature, is that the extant FRAND rules are generally useful, but tend to be inadequate because they are imprecise and leave unresolved such critical issues as (a) the meaning of a reasonable royalty, even conceptually; (b) the meaning of “non-discriminatory;” (c) to whom licenses must be offered; and (d) under what circumstances may a SEP holder obtain an injunction.84 These imprecise FRAND commitments are therefore not sufficient to adequately prevent ex post opportunism. The recent revisions to IEEE’s FRAND policy represent a signiﬁcant step in the right direction, but even this advance leaves important questions unanswered.85 If FRAND rules are inadequate in these ways, litigation involving extant FRAND rules would likely be resolved only at the ﬁnal, fourth step. The defendant would be able to demonstrate the beneﬁts created by the standard; the plaintiff would be able to demonstrate the creation of market power and that other reasonable and practical rules or policies would ameliorate the problem. The case would thus turn on whether the defendant is able to demonstrate that signiﬁcant beneﬁts associated with standardization could not have been realized if the SSO had adopted those other rules or policies.

The court would have available a variety of possible remedies if the plaintiff prevails. Implementers that paid supracompetitive royalties or were unlawfully excluded in whole or in part from product markets as a result of the inadequate FRAND policies would be entitled to damages and, in some cases, to treble damages.86 If the unlawful SSO conduct is regarded as the collective action of the SSO and its members, which is likely to be the case in most instances, SSO members would be jointly and severally liable for the damages. Forward-looking injunctive relief aimed at restoring competition would need to be fashioned to the requirements of the individual case. For example, a court could order the SSO to adopt a new rule or policy proposed by the plaintiff. If the court is reluctant to take on that governance role, it might give the SSO a period of time—maybe ninety days—to develop a rule, subject to the court’s ultimate approval, which would adequately ameliorate the competitive problem created by the SSO. Alternatively or in addition, the court might order the parties to attempt to negotiate a rule or policy on which they can agree. And, depending on the circumstances, the court might order SEP holders, including at least those that were defendants in the case, to comply with the new SSO rules and policies.

#### Threatening antitrust liability lures SSO’s into adopting best practices.

Lemley & Shapiro 13, \*Mark Lemley is the William H. Neukom Professor at Stanford Law School and a partner at Durie Tangri LLP; \*Carl Shapiro is the Transamerica Professor of Business Strategy at the Haas School of Business, University of California at Berkeley and a Senior Consultant at Charles River Associates; (2013, “A SIMPLE APPROACH TO SETTING REASONABLE ROYALTIES FOR STANDARD-ESSENTIAL PATENTS”, (https://faculty.haas.berkeley.edu/shapiro/frand.pdf)

Under our approach, many of these issues should become moot, since the patentee cannot obtain an injunction (or transfer the patent to someone who can) against a willing licensee, and since competitors are not involved in jointly setting the reasonable royalty rate. If SSOs set clear, reasonable rules following the best practices we recommend, and parties follow those rules, there should be little or no need for antitrust to intervene. Indeed, even the risk of non-disclosure of a patent is lessened, since the patentee has committed to license its essential patents whether or not it discloses them. For the most part, the rules we have described are self-executing, meaning that even if a party tries to break the rules set by the SSO there still may be no need for antitrust to intervene. Thus, we suggest that parties who abide by these procedures—patentees, implementers, and the SSOs themselves—should be immune from antitrust liability for activities that merely follow those rules.107 They have entered into an arrangement that is on balance good for competition, one that allows patentees to receive reasonable royalties but prevents holdup and reduces the risk of monopolization by trickery.

The fact that antitrust remains a last resort available when SSOs don’t follow best practices may have two practical benefits, however. First, under our approach the promise of avoiding the risk of antitrust liability will be a powerful incentive for both SSOs and patent owners to adopt the best practices we propose. Second, the risk of antitrust liability may be relevant when an individual patentee wants to adopt best practices but the SSO governing the standard has not yet done so. We propose that a patentee that unilaterally commits to the FRAND procedures we describe here should be immune from antitrust liability for following these procedures.108 A patentee’s unilateral binding commitment to arbitration could be enforced whether or not it was elicited by an SSO. Thus, just as the prospect of antitrust immunity might lure SSOs to adopt best practices, it might also lure patentees to implement those practices even if the SSO has not done so. Given the large number of standard-essential patents based on preexisting standards,109 and given that SSOs tend to update their IP rules rather slowly,110 this is not a small matter.

#### \*\*\*Only antitrust enforcement creates a consumer-action feature that counterbalances SSO’s conspiratorial incentives---private action fails.

Melamed & Shapiro 18, \*A. Douglas Melamed is Professor of the Practice of Law at Stanford Law School; \*Carl Shapiro is the Transamerica Professor of Business Strategy at the Haas School of Business at the University of California at Berkeley; (May 2018, “How Antitrust Law Can Make FRAND Commitments More Effective”, <https://www-cdn.law.stanford.edu/wp-content/uploads/2018/05/How-Antitrust-Law-Can-Make-FRAND-Commitments-More-Effective.pdf>)

2. Why Antitrust Enforcement Is Necessary

Some SSO members have an interest in ensuring that the SSO takes steps to minimize the potential harms from the SEP holders’ monopoly power, and this undoubtedly explains in part why most SSOs have adopted FRAND policies or similar requirements. But, as shown in the economic model in the Appendix,73 SSOs cannot in general be counted on to adopt effective FRAND policies. The bases for this conclusion, which is central to our argument for the applicability of Section 1 to SSO FRAND rules, can be summarized as follows.74

First, the SSO members collectively have an interest in permitting SEP holders to charge supracompetitive royalties that elevate the downstream price of compliant devices to the monopoly level. Doing so will enable the members in aggregate to collect increased revenues from consumers, and thus to generate increased profits that in theory could be shared by all the members. In other words, supracompetitive royalties can enrich industry participants as a group at the expense of final consumers. This fact alone should serve as a clear and strong signal regarding the dangers of counting on SSOs to implement effective FRAND policies: if the SSO members negotiate efficiently, the outcome will be just as bad for consumers as if the members agreed to fix downstream prices.75 The fundamental problem is that final consumers are not at the table when the SSO rules are negotiated.

Second, SSO members that own SEPs but earn little or no profits as implementers have a powerful self-interest in being able to exercise the ex post monopoly power associated with their SEPs. Because SSO policies are usually determined by a consensus process, these members will likely be able to block the adoption of fully effective FRAND policies. Moreover, these SSO members often have the greatest interest in SSO patent policies. Since much of their income may be attributable to patent licensing, they can be expected to devote substantial resources to block the adoption of FRAND policies that effectively prevent patent holdup.

Third, even SSO members that earn significant profits as implementers may have mixed incentives if they also own SEPs, which can also lead to weak or in-effective FRAND rules. In the Appendix, we show that, if the requisite share of votes in the SSO are cast by firms whose share of SEP royalties is at least as large as their share of downstream profits, and if these firms can coordinate their voting over the FRAND rules, then an SSO unconstrained by antitrust laws will establish FRAND rules leading to an outcome no better for consumers than would result from an integrated monopolist controlling all SEPs and all downstream sales.76

Fourth, even SSO members that are downstream implementers and own few, if any, SEPs may have only a modest interest in promoting effective policies to restrict ex post opportunism. Because all implementers will be subject to the opportunism, all of them will face increased licensing costs, and therefore will likely be able to pass on most or all of the increased costs to their customers.77 Furthermore, these implementers might not be especially active or effective in the standard-setting process for free-riding or public-good reasons, especially if SEP royalties constitute only a relatively small portion of the costs of their standard-implementing products. Public choice theory predicts that the highly motivated SEP holders are likely to have the greatest influence over patent policies.

Empirical evidence bears out these concerns. As a starting point, we find it striking that SSO FRAND rules are almost always quite vague.78 Notably, SSOs in which SEP holders are more prevalent tend to have weaker FRAND rules.79 Further, to our knowledge, SSOs have made almost no effort to enforce their FRAND rules and have, instead, left enforcement efforts to others.80 This evidence raises serious doubts about the effectiveness of the existing FRAND rules in preventing ex post opportunism.

# 2AC

## Adv — Innovation

#### No bioterrorism -- complexities

Revill, 17 - Research Fellow with the Harvard Sussex Program at SPRU (Dr. James Revill, “Past as Prologue? The Risk of Adoption of Chemical and Biological Weapons by Non-State Actors in the EU,” *European Journal of Risk Regulation*, pages 626-642, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/6B824CDE0E25FD86AC3D0BD07822A743/S1867299X17000356a.pdf/div-class-title-past-as-prologue-the-risk-of-adoption-of-chemical-and-biological-weapons-by-non-state-actors-in-the-eu-div.pdf

The second factor is “the perceived complexity of the innovation in terms of adoption and use”.40 This is important in the innovation literature, as Rogers remarked, “[t]he complexity of an innovation, as perceived by members of a social system, is negatively related to its rate of adoption”.41 Several scholars of terrorist innovation have also highlighted the issue of complexity;42 or, as Cragin et al have stated, “[h]ow simple or complex a technology appears affects perceptions of how risky it will be to adopt.”43

In most cases terrorist groups appear to have largely opted for the simplest pathway towards the achievement of their goals and the weapons used tend to be vernacular, functional devices drawing on local and readily-available materials, rather than sophisticated, “baroque” technologies. This is certainly the case with IEDs, the history of which is characterised largely by incremental innovations – although nevertheless frequently effective ones – with many means of delivery recycled from the past.44 Complexity can therefore be seen as important in the adoption of technology by terrorists generally, but is perhaps particularly acute in the case of CBW technology.

Some CBW can be relatively simple: “chlorine-augmented, vehicle-borne IEDs,” as employed by Al-Qaeda in Iraq (AQI) from 2006 to 2007 are not sophisticated weapons.45 Attacks on chemical production facilities, an apparent tactic of Serbian forces in the early to mid-1990s,46 employed relatively simple technologies – specifically explosives – with toxicity a secondary by-product. Direct contamination of food,47 drink48 or healthcare products49 does not require particularly sophisticated technology for the purposes of delivery – although may require some considerable skill to culture and scale-up a biological agent – and has been a common approach in European CBW incidents.50 Similarly, the contamination of water systems, something familiar to Europe,51 can also be relatively easily attempted. However, in most cases such methods of dissemination have generated results that are far short of the “mass destruction” that CBW are associated with, although this does not mean such a possibility can be ignored by those working on public health preparedness.

Although some relatively simple approaches could cause significant harm, mass casualty attacks still require considerable expertise, something particularly acute in the context of biological weapons.52 The most effective route to weaponising biology is arguably through the process of aerosolising agents, something recognised mid-way through the last century as opening up the theoretical possibility of using biological weapons on a gigantic scale.53

However, realising such theoretical potential is difficult and it took states decades to develop more predictable biological weapons,54 and even then such weapons were acutely vulnerable to environmental factors.55 For non-state groups such complexity has proven a significant barrier to CBW development. By means of an example, one of the best-resourced biological weapons programs, that of Aum Shinrikyo, failed variously because the group acquired the wrong strain, contaminated fermenters and were faced with insurmountable production and dissemination difficulties.56 There are of course exceptions, such as the 2001 anthrax Letter Attacks in the US. However, if one accepts the conclusions of the FBI that this sophisticated attack with aerosolised anthrax in the US postal system was perpetrated by a US biodefence researcher, Dr Bruce Ivins,57 it is an exception that proves the rule.

To circumvent the difficulties with aerosolisation, arguably one could use human-to-human transmissible biological agents as part of a suicide bioterror operation. There are good reasons for concern over how crude suicide bioterrorists could employ such a tactic. However, the use of highly contagious agents is also poorly predictable and would have to deal with social factors, such as the “spatial contact process among individuals”, which can spell “out the difference between large-scale epidemics and abortive ones”.58

The counter to this argument is the growing access to data and the changing human geography of the life sciences. Some 83% of European households reportedly are online, effectively allowing access to what is a growing body of available data on CBW, including so-called bioterrorist “recipes” and “blueprints” that are available in both mainstream scientific as well as more subversive literatures online. It is also clear that there is a changing human geography in European life sciences (for peaceful purposes), with the emergence of 30 DIY-bio groups located in Europe59 and some 80 European teams in the international Genetically Engineered Machines (IGEM) competition in 2016.60 This is compounded by reports that groups such as Daesh have deliberately sought to recruit foreign fighters “including some with degrees in physics, chemistry, and computer science, who experts believe have the ability to manufacture lethal weapons from raw substances”.61

Whilst it would be unwise to ignore such developments, there is a need for caution in looking at the extent to which new technologies and geographies will facilitate the adoption of chemical and biological weapons by groups seeking to target European countries. First, data is not information, and information is not knowledge, let alone the tacit knowledge required for CBW.62 In many cases a degree of determination and dedication will be required merely to separate online fantasy from fact and identify operationally useful information (of relevance to the European context) from nonsense (or information pertinent to contexts other than Europe). Second, with new technologies there is the potential for such tools to enable some, but certainly not all, actors, and even then new technologies bring new challenges. CRISPR, gene editing technology is currently seen as a particular source of promise and peril, which purportedly enables “even largely untrained people to manipulate the very essence of life”.63 As much may be technically true, yet “untrained people” would nonetheless require some guidance in identifying suitable areas of genetic structures to manipulate. Moreover, CRISPR would only get aspiring weaponeers so far, with the process of culturing, scaling-up and weaponisation still requiring considerable attention and interdisciplinary skills, typically generated through “large interdisciplinary teams of scientists, engineers, and technicians”,64 in order to be effective.

Indeed, for all the progress in science and technology, biological weapons are still not used, in part, because of the complexity of such weapons; and the chemical weapons that are used today are largely the same as the chemical weapons of 100 years ago. As Robinson noted “It remains the case today that, in the design of CBW, increasingly severe technological constraint sets in as the mass-destruction end of the spectrum is approached: the greater and more assured the area-effectiveness sought for the weapon, the greater the practical difficulties of achieving it”.65

#### Chinese control of tech governance undermines global strategic stability---causes global conflict.

**Jain 19**, senior fellow with the Scowcroft Center for Strategy and Security, where he oversees the Atlantic Council’s Democratic Order Initiative and D10 Strategy Forum; and Matthew Kroenig, deputy director for strategy in the Scowcroft Center for Strategy and Security and associate professor of government and foreign service at Georgetown University (Ash, “Present at the Re-Creation: A Global Strategy for Revitalizing, Adapting, and Defending a Rules-Based International System,” *Atlantic Council*, <https://www.atlanticcouncil.org/wp-content/uploads/2019/10/Present-at-the-Recreation.pdf>)

The system must also be adapted to deal with new issues that were not envisioned when the existing order was designed. Foremost among these issues is emerging and disruptive technology, including AI, additive manufacturing (or 3D printing), quantum computing, genetic engineering, robotics, directed energy, the Internet of things (IOT), 5G, space, cyber, and many others. Like other disruptive technologies before them, these innovations promise great benefits, but also carry serious downside risks. For example, AI is already resulting in massive efficiencies and cost savings in the private sector. Routine tasks and other more complicated jobs, such as radiology, are already being automated. In the future, autonomous weapons systems may go to war against each other as human soldiers remain out of harm’s way. Yet, AI is also transforming economies and societies, and generating new security challenges. Automation will lead to widespread unemployment. The final realization of driverless cars, for example, will put out of work millions of taxi, Uber, and long-haul truck drivers. Populist movements in the West have been driven by those disaffected by globalization and technology, and mass unemployment caused by automation will further grow those ranks and provide new fuel to grievance politics. Moreover, some fear that autonomous weapons systems will become “killer robots” that select and engage targets without human input, and could eventually turn on their creators, resulting in human extinction. The other technologies on this lisgt similarly balance great potential upside with great downside risk. 3D printing, for example, can be used to “make anything anywhere,” reducing costs for a wide range of manufactured goods and encouraging a return of local manufacturing industries.61 At the same time, advanced 3D printers can also be used by revisionist and rogue states to print component parts for advanced weapons systems or even WMD programs, spurring arms races and weapons proliferation.62 Genetic engineering can wipe out entire classes of disease through improved medicine, or wipe out entire classes of people through genetically engineered superbugs. Directed-energy missile defenses may defend against incoming missile attacks, while also undermining global strategic stability. Perhaps the greatest risk to global strategic stability from new technology, however, comes from the risk that revisionist autocracies may win the new tech arms race. Throughout history, states that have dominated the commanding heights of technological progress have also dominated international relations. The United States has been the world’s innovation leader from Edison’s light bulb to nuclear weapons and the Internet. Accordingly, stability has been maintained in Europe and Asia for decades because the United States and its democratic allies possessed a favorable economic and military balance of power in those key regions. Many believe, however, that China may now have the lead in the new technologies of the twenty-first century, including AI, quantum, 5G, hypersonic missiles, and others. If China succeeds in mastering the technologies of the future before the democratic core, then this could lead to a drastic and rapid shift in the balance of power, upsetting global strategic stability, and the call for a democratic- led, rules-based system outlined in these pages.63

#### Deterrence is necessary and works---negative evidence selectively reads Chinese actions.

Edel 18, Non-Resident Senior Fellow at the United States Studies Centre at the University of Sydney, (Charles, 2018, “Limiting Chinese Aggression: A Strategy of Counter-Pressure”, https://www.the-american-interest.com/2018/02/09/limiting-chinese-aggression-strategy-counter-pressure/#\_ftnref18)

Counter-Pressure Works

Finally and most critically, it is simply not true that China cannot be deterred and is, sooner or later, bound to dominate the region. The size and capability of the American military still deter outright military conflict between China and the United States and its treaty allies in the Asia-Pacific region. Everyone knows that, so the present situation is not the issue. The issue is the path to the future, and it is here that Beijing has chosen an asymmetrical approach to achieving its aims—specifically by working to develop “gray zone” operations.[[10]](https://www.the-american-interest.com/2018/02/09/limiting-chinese-aggression-strategy-counter-pressure/#_ftn10)

Note, for example, Chinese actions in the South China Sea.[[11]](https://www.the-american-interest.com/2018/02/09/limiting-chinese-aggression-strategy-counter-pressure/#_ftn11) Advances have been taken slowly and in disparate locations. They are usually first probed not by visible state-forces, but by seemingly private actors; and they are justified in shifting and ambiguous language. The result is a complicated incremental assault on the status quo. Meanwhile, if the United States and its allies act first to blunt such “precedent creep,” they open themselves to the charge of needlessly provoking the revisionist power.[[12]](https://www.the-american-interest.com/2018/02/09/limiting-chinese-aggression-strategy-counter-pressure/#_ftn12) But if they wait too long, they will confront a degraded security environment, increased questions about their commitment and credibility, and concerns that they have surrendered the initiative.

But for all the questions that Chinese probes have raised, the proposition that China is undeterrable, rather than undeterred to date, stands badly in need of testing. This assumption is based on a highly selective version of recent history that minimizes effective counter-pressure efforts, exaggerates Chinese strengths and resolve, and fails to note Beijing’s weaknesses. Finally, to assume that concerted counter-pressure, discriminately applied, will have no discernible effect on Beijing’s calculations is preemptively to concede not only the initiative on policy, but also an ever-enlarging Chinese sphere of influence in the region—for absent U.S, leadership, the other regional powers, their collective clout notwithstanding, will have a hard time concerting their efforts.

Far from being undeterrable, recent history suggests a much more varied picture of China. When Beijing perceives that its actions are unlikely to cause pushback or counter-pressure, it has continued pushing. But when Chinese activities have been met with concentrated counter-pressure, the response has not been predictably escalatory. Just note: Japan’s response to the PRC’s ham-handed rollout of an ADIZ (Air Defense Identification Zone) in the ECS in 2013; South Korea’s refusal to bow to Chinese economic pressure over the deployment of THAAD as a defense against DPRK ballistic missiles; President Obama’s 2015 threat to impose sanctions in response to Chinese state-sponsored cyber activities; and Obama’s purported drawing of a redline around the reclamation of Scarborough Shoal to Xi Jinping in March 2016. While it’s unclear who saved face and who lost face in Doklam, India’s response to Chinese activities in Bhutan caused neither war nor acquiescence to Chinese probes. Similarly, Vietnam’s 2014 response to the Chinese oil rig operating in its waters, and China’s withdrawal of the rig, demonstrate that Beijing was willing to recalibrate, if not withdraw, its activities when met with a resolute response. Finally, for all the hand-wringing that accompanied the debate about a quadrilateral arrangement between India, Japan, Australia, and the United States, Beijing’s actual reaction has been muted.

The same goes in the economic realm. In 2012, Washington imposed sanction on the China-based Bank of Kunlun for its dealings with Iran. Yet despite Chinese warnings that such a move would sour bilateral relations and undercut Beijing’s support for curbing Tehran’s nuclear ambitions, Beijing offered merely a formulaic protest, directed the bank to cease its activities, and continued cooperation with the United States. With respect to secondary sanctions at least, a high-ranking Obama official who was in charge of implementing such sanctions concluded that, despite the fears of a furious Chinese reaction and calls for caution, “history teaches that we should not worry too much about an adverse Chinese reaction.”[[13]](https://www.the-american-interest.com/2018/02/09/limiting-chinese-aggression-strategy-counter-pressure/#_ftn13)

The actual, as opposed to the imagined, record of Chinese responses suggests that Beijing’s reaction is as dependent on how others respond as it is on what they wish to achieve. It also implies that Chinese pressure is carefully calibrated to fit, but not necessarily exceed, any given situation. China will not always roll over and play dead when confronted with counter-pressure; it depends on what it thinks is at stake and what counter-pressure indicates about the intentions of others. Note, however, what happens no counter-push exists. China has not only manufactured features in the South China Sea, but has continued its push to build out its infrastructure and rotate military assets on them. Faced with the menace of increased activity around Scarborough Shoal, while being dangled the promise of Chinese economic largesse, the Philippines, under Rodrigo Duterte, has ceased protesting Chinese activities. And by using Cambodia and Laos and now the Philippines to undermine any unanimity in ASEAN, ASEAN has not even been able to condemn Chinese bullying by name.

Chinese policymakers have demonstrated a logical aversion to conflict. They do not want to put the regime’s stranglehold on Chinese society at risk or do things that harden the existing American alliance structure into something more multilateral and more offensively directed against Beijing. As a result, Chinese actions are less reckless gambles than premeditated probes.[[14]](https://www.the-american-interest.com/2018/02/09/limiting-chinese-aggression-strategy-counter-pressure/#_ftn14) When the reaction has been formidable, Chinese activities have been recalibrated.

#### Chinese global governance is an authoritarian ruse---they cannot and will not replicate liberal ideals because doing so would undermine power consolidation.

Hart & Johnson 19, \*Melanie Hart is a senior fellow and director for China Policy at the Center for American Progress. She is responsible for formulating CAP policy proposals on China and U.S.-China relations and leading CAP efforts to promote those proposals with political leaders in the United States and Asia; \*Blaine Johnson serves as a policy analyst for National Security and International Policy at the Center for American Progress; (February 28th, 2019, “Mapping China’s Global Governance Ambitions”, https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/)

Beijing intends to weaken liberal democratic principles and augment or replace them with authoritarian governance principles

Chinese leaders recognize that in order to continue advancing economically, they cannot wall off China’s economy or society from the global community. However, integrating with a global system that values liberal principles over authoritarian ones brings sizable risk, because it exposes Chinese citizens to a set of ideals, standards, and benefits their current leaders do not intend to meet or provide. To address this risk, Chinese leaders are seeking to make the international system more like China. This is the opposite of what Western nations intended when they brought China into that system.

In the United States and other Western nations, there is a tendency to avoid framing disputes with China in ideological terms, which is generally viewed as veering toward dangerous Cold War thinking. On the Chinese side, however, Chinese leaders frequently claim that their nation is fighting an ideological battle against Western values—particularly freedom, democracy, and human rights—which, from a Western perspective, are universal values that should apply equally to all citizens. As a repressive authoritarian regime, Beijing does not want Chinese citizens to judge their own leaders using those standards. Where those standards exist in the global governance system, Beijing views them as a fundamental security threat.

President Xi outlined those fears at the 2013 National Propaganda and Ideological Work Conference in Beijing when he described Western nations as “hanging up a sheep’s head while selling dog meat.”[11](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-11) By that, he was intimating that Western nations were engaging in false advertisement, making self-righteous claims about promoting universal values for the sake of humanity when their real purpose was, in his words, “to fight with us for positions, fight over the will of the people, fight over the masses, and ultimately overthrow the leadership of the Communist Party of China.”[12](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-12) A few years later, at a 2015 work conference at the Chinese Communist Party Central Party School, President Xi warned that among nations who fall for the universal values trap, “some have been tormented beyond recognition, some have split up into pieces, some have been enveloped in flames of war, some are noisy and in disarray all day.”[13](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-13) He pointed to Syria, Libya, and Iraq as prime examples.

To avoid that fate, President Xi has called, and continues to call, on China to use its own “discourse power” to push back against universal values in the global governance space.[14](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-14) Still, at first glance, some of President Xi’s international statements appear to support liberal values. For example, in a 2017 speech to the United Nations, Xi claimed that China’s aim is to “build an open and inclusive world” and that Beijing believes “diversity of human civilizations … drives progress of mankind.”[15](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-15) What Western observers need to understand, however, is that when Chinese foreign policy experts unpack that statement, they view it as a call for political diversity where authoritarian systems and values have global status equal to liberal democratic ones.[16](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-16) For example, writing on internet freedom, People’s Liberation Army Major General Hao Yeli writes that the global system should “avoid the excessive pursuit of unregulated openness, in order not to cross a tipping point beyond which global cultural diversity is subordinated to a single dominant culture.”[17](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-17) Similarly, Han Zhen, secretary of the Beijing Foreign Studies University Chinese Communist Party Committee, calls for a global pivot away from “Western centrism,” which he defines as a form of “cultural absolutism” that seeks to hold China and other nations accountable to Western liberal democratic standards.[18](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-18) Echoing President Xi’s call for diversity, Han writes: “It is imperative to make more people realize the ‘universal values’ that have long been lauded by Western societies are actually a duplication of Western political, economic, social, and cultural models … human society should extricate itself from the vicious circle of Western-centrism and build a system of values that is characterized by mutual learning and mixing between diverse groups.”[19](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-19)

Xi’s oft-stated call for a “community of common destiny for mankind” is part of this effort to give authoritarian principles more sway in the global governance system.[20](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-20) In a liberal democratic order, individuals have inalienable rights that the state cannot take away. In China’s preferred authoritarian order, collective rights and interests—so-called mankind—are more important than individual rights and interests, and the state speaks on the collective’s behalf to determine its interests. Beijing is trying to convince the global community that authoritarian systems are better than democracies in this regard. Zhang Weiwei, dean of the China Institute at Fudan University, lays out that argument in the Chinese Communist Party political journal Qiushi, writing:

The biggest difference between the institutional arrangements of China and Western countries is that the former has a political force representing the people’s collective interest and the latter do not. In the West, different political parties represent the interest of different social groups. As a result, national policies are constantly wavering, political parties and interest groups are frequently engaged in bigger conflict with each other, and national development easily loses direction. In contrast, the CPC is a political party dedicated to serving the people wholeheartedly, and one that has played the role of leader, regulator, and coordinator throughout China’s modernization drive.[21](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-21)

Moreover, Zhang argues that the same dynamic applies at a global level: The Chinese model can effectively address complex problems that a democratic policymaking process cannot. Since he views the Chinese model as superior, Zhang calls on China to put forward “a series of Chinese solutions to difficult issues in global governance.”[22](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/#fn-466768-22) When President Xi calls for a “community of common destiny for mankind,” he is pushing a new vision for global governance in which the state, not the individual, is always the ultimate authority.

## Adv — Cyber

## CP — Antitrust PIC

#### Permutation do the counterplan---the counterplan still expands the scope of core antitrust laws by increasing prohibitions.

Bradford and Chilton 18 (Anu Bradford, Henry L. Moses Professor of Law and International Organization, Columbia Law School. Adam S. Chilton, Assistant Professor of Law and Walter Mander Research Scholar @ the University of Chicago. “Competition Law Around the World from 1889 to 2010: The Competition Law Index” , Columbia Law School Scholarship Archive Faculty Scholarship, <https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=3519&context=faculty_scholarship> , 2018, date accessed 9/5/21)

The Scope Index is the closest to the CLI in that it also measures the law in the books, treating prohibitions as elements that increase the scope (or stringency) of the law and defenses as elements that reduce the scope (or stringency) of the law. Basic categories in the Scope Index and our CLI are also the same, even if somewhat differently labeled. For example, we refer to “anticompetitive agreements” where the Scope Index refers to “restrictive trade practices.”

#### 2---competition-specific expertise---DOJ and FTC enforcement are key. Even if other agencies are granted authority to regulate, they will underenforce.

Dogan 08, \*Stacey L. Dogan, Professor of Law, Northeastern University; \*Mark Lemley, William H. Neukom Professor, Stanford Law School; of counsel, Keker & Van Nest LLP; (October 2008, “Antitrust Law and Regulatory Gaming”, https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1873&context=faculty\_scholarship)

I. The Relative Efficiency of Antitrust and Regulation

The growing antitrust deference to regulation is cause for concern. Both antitrust and regulation are economic responses to market failures.46 Implemented correctly, both are designed to serve the ends of economic efficiency.47 It is therefore reasonable to judge the relative efficacy of antitrust and regulation by economic criteria. And judged by those criteria, virtually all economists would agree that antitrust-overseen market competition is superior to industry regulation. In particular, none of the arguments the Court has offered as a reason to prefer regulation to antitrust withstand scrutiny.

Relative expertise.

It is true, as the Court emphasized in Trinko and Credit Suisse, that antitrust courts are generalist courts, while regulatory agencies tend to specialize in a particular industry and its problems. That specialization should, all other things being equal, mean that expert regulators will do a better job than judges or juries of reaching the right result. But other things are far from being equal. Antitrust courts have two significant advantages over regulatory agencies when it comes to promoting competition.

First, antitrust courts are trying to promote economic efficiency, while regulators often aren’t. For decades, efficiency has served as the sole criterion on which to judge antitrust rules. And courts have had over a century in which to hone those rules to achieve that end. Without question, courts have made mistakes in the past. But there is a strong consensus among antitrust scholars that the wave of cases in the last 30 years has largely moved antitrust in the right direction, eliminating any significant risk that antitrust enforcement will do more harm than good.48 Scholars may fight over whether a Chicago School or a post-Chicago School approach will achieve the right result in specific cases,49 but for the most part they are tinkering at the margins: the law and the scholarship have converged with respect to both the proper goals of antitrust and the general rules that will achieve those goals.

Regulation, by contrast, is frequently not even intended to achieve economic efficiency through competition. Occasionally that is because of a legislative judgment that competition is impossible, though the number of industries thought to be natural monopolies for which markets won’t work has shrunk dramatically in the past four decades.50 Industry regulation that excludes entry in order to promote a natural monopoly, as telephone regulation did before 1984, is not likely to achieve a competitive outcome.

More often, the goals of the legislators who establish regulatory agencies, or the goals of the regulators who run those agencies, are to achieve something other than competition. Indeed, many regulations are aimed precisely at eliminating competition, as was the government- sponsored raisin cartel in Parker v. Brown51 or any of its modern descendent crop-support programs administered by the Department of Agriculture. It should be obvious that regulations intended to reduce competition will not promote it. But even if the regulation is not directly inimical to competition, competition is frequently irrelevant to, or at best a minor consideration in, a regulator’s agenda. Regulators may care about the safety and efficacy of a drug, for example, and only incidentally about whether there is competition in the sale of that drug. They may seek to reduce traffic deaths or air pollution by mandating technology, regardless of the effect that mandate has on the price manufacturers can charge or the number of products they sell. These are laudable goals, to be sure, but they are not competition-related goals. An agency tasked with achieving these goals is likely to ignore threats to competition from the industry it regulates so long as those threats do not compromise its core mission. Thus, the state and local governments that enacted the privately-drafted National Fire Protection Code at issue in Allied Tube into law were interested in stopping fires; doubtless they thought little if at all about the competitive effects of the code, even though it turned out that the code was drafted by interested private parties with the purpose of impeding competition rather than promoting fire safety.52

Even those agencies whose mission expressly involves consideration of competition issues will not necessarily make it their first among potentially conflicting priorities. The SEC, for example, which as Justice Breyer pointed out is dedicated to improving market information and expressly considers competition among other issues in setting regulation,53 is first and foremost an investor-protection and information-disclosure agency, not an agency that investigates and weeds out cartels or other anticompetitive practices. It is unlikely to devote much in the way of time or resources to such issues, because even if it is tasked to consider such issues they do not reflect the agency’s primary purpose. Similarly, even an agency like the Federal Communications Commission that is directly focused on competitive conditions in a particular market may naturally pay attention primarily to that market, and give less if any attention to the effect its rules might have on competition in adjacent markets or competition from unanticipated new businesses. This arguably explains the FCC’s willingness to largely ignore the effects of its decisions on the Internet, for example: it is telecommunications, not the Internet, that the FCC is tasked to regulate.

Agencies that view competition as secondary, or view it through the lens of a particular industry’s characteristics and interests, are less likely to create and enforce rules that optimally encourage competition.54 At a bare minimum, therefore, the industry-specific expertise of an agency must be balanced against the competition-specific expertise of the specialist antitrust agencies: the Federal Trade Commission (FTC) and the Department of Justice Antitrust Division.

#### 3---regulatory capture---even honest agencies will subject to lobbying and industry pressure that diverts the counterplan’s purpose. Antitrust courts are superior and impartial.

Dogan 08, \*Stacey L. Dogan, Professor of Law, Northeastern University; \*Mark Lemley, William H. Neukom Professor, Stanford Law School; of counsel, Keker & Van Nest LLP; (October 2008, “Antitrust Law and Regulatory Gaming”, https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1873&context=faculty\_scholarship)

The problem with agencies is much greater than just their questionable mandate to promote competition, however. Agencies are famously subject to “capture” by the industries they are supposed to regulate.55 That capture can take many different forms. Sometimes regulators or legislators are captured in the most venal sense – they are bribed or otherwise given personal benefits in exchange for voting a particular way. This seems to have been the case in Omni Outdoor Advertising, for example. Regulators who accept bribes (or politicians who accept campaign contributions in exchange for a particular vote) are not acting in the public interest but in their private interest, a private interest that necessarily aligns with the industry participant doing the bribing. Even a regulator who would never accept bribes may still seek to maximize, not the public interest, but his own power or the power and interests of his agency, a fact that industry can often use to its advantage.

Capture need not be so brazen, however. Even honest regulators and legislators can be captured through the mechanism of public choice theory.56 A legislator that tries to maximize her constituents’ expressed preferences may still end up supporting legislation that benefits private firms at the expense of the public interest, because the private firms will frequently have a concentrated interest – and therefore show up to lobby on a particular issue – while the public is hard to organize even around issues that may affect a great many of them diffusely. Regulators are subject to the same effect. A notice and comment rulemaking is likely to produce more comments from people with a concentrated interest in the outcome, and fewer comments from those with a more diffuse interest. Thus, regulators who try in good faith to determine what the public thinks of a particular regulation may still end up with a skewed view of the pros and cons. This may be particularly likely with competition issues. While the public as a whole has a strong interest in unfettered competition, any individual member of the public is unlikely to be affected much by a particular regulatory decision. And particularly where the industry as a whole colludes to seek regulatory intervention that benefits them, as in Ticor Title, there are unlikely to be competitors who can stand as proxy for the interests of the public.

Finally, even legislators and regulators aware of the existence of public choice problems and determined to do the right thing are still susceptible to forms of what we might call “soft” capture. Acquiring accurate information about market conditions is often very difficult, for example. Companies with a vested interest in the outcome can hire lobbyists that provide information helpful to their side, and a regulator who cannot get information except from those lobbyists may have little choice but to accept that information as true. Even if there are competing sources of information, interested parties can and do hire as lobbyists former employees, colleagues, or friends of the regulator, and it is natural human instinct to trust those people more than strangers. And regulators tend to come from the industries they regulate, which may mean that they start out seeing things from the industry’s perspective.

Judges, by contrast, are much less subject either to having their purpose diverted or to capture. While some have tried to argue that judges face some of the same interest group constraints as legislators and administrative agencies,57 the fact is that antitrust courts are trying to achieve the goal of economic efficiency, they are doing it in industries in which they have no direct financial interest, they cannot act to benefit their “agency” in rendering a decision, and the structure of the litigation process helps ensure to the extent possible that both sides are presented in a relatively balanced way. Courts aren’t perfect, of course. But all advantages are comparative, and the fact that antitrust courts are trying to promote competition rather than to achieve some other end (whether legislated or self-motivated) provides a powerful counterweight to the industry expertise of administrative agencies. It is important to keep in mind, as Areeda and Hovenkamp summarize, that “it often turn[s] out that the principal beneficiaries of industry regulation were the regulated firms themselves, which were shielded from competition and guaranteed profit margins.”58 Courts should not assume that regulation will lead to competition merely because regulators know more than courts about the industries they regulate.

#### That’s especially true in the standard-setting context---regulatory gaming exacerbates monopoly pricing.

Dogan 08, \*Stacey L. Dogan, Professor of Law, Northeastern University; \*Mark Lemley, William H. Neukom Professor, Stanford Law School; of counsel, Keker & Van Nest LLP; (October 2008, “Antitrust Law and Regulatory Gaming”, https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1873&context=faculty\_scholarship)

2. Evading regulatory limits as antitrust harm

The second open question is whether antitrust injury occurs when a defendant’s misrepresentations prevent an agency from placing limits on an exercise of market power, rather than eliminating the market power altogether. In Rambus v. FTC,148 the D.C. Circuit effectively held that where market power resulted from a regulatory decision (there, the grant of a patent), antitrust law could not constrain the price the monopolist charged. Rambus involved alleged misrepresentations made in the course of a private standard-setting organization’s deliberations. The FTC claimed that Rambus had withheld material information about patent rights that it held over the relevant technology. The FTC alleged that if the SSO had known about Rambus’s patents, either it would have adopted a different standard, or it would have demanded some form of fair and nondiscriminatory licensing terms on Rambus’s patents. The D.C. Circuit found the second allegation legally inadequate, concluding that the mere exercise of market power (i.e., charging higher prices) does not violate the antitrust laws if the market power itself arose from a valid government grant.149

The Rambus court relied on NYNEX v. Discon,150 in which the Supreme Court refused to apply the per se rule to a kickback scheme involving a regulated utility. The regulated party in Discon awarded a contract for non-regulated services to a company that would charge higher prices that the regulated company could then pass on to consumers through rate regulation. The NYNEX Court rejected an antitrust claim alleging that the scheme constituted an unlawful group boycott, absent proof that it harmed competition (not just a competitor) in the non-regulated service market. The Court specifically acknowledged that consumers were injured by the conduct, because it resulted in higher prices in the regulated market. Because that injury came from the exercise of agency-granted market power, however, the Court deemed it beyond the reach of antitrust law. While NYNEX itself involved only the question of whether the per se rule applied, Rambus read it as going further and immunizing any conduct that owed its origin to a regulatory grant of market power.

Both NYNEX and its substantial new extension in Rambus are problematic as matters of antitrust law. The harm to competition in NYNEX did not stem solely from government-granted market power; it stemmed from the defendant’s effort to extend that market power in ways that deceived the regulatory agency and prevented it from controlling NYNEX’s behavior. Similarly, the harm to competition in Rambus did not stem solely from the government’s grant of a patent, but from the combination of that grant with Rambus’s deception of a standard-setting organization that would otherwise have restrained the ability of Rambus to charge a supracompetitive price for that patent. Both of these cases, in other words, involve deliberate and effective regulatory gaming. By refusing to apply antitrust law to private deceptive conduct that manipulates a regulatory process, or extends or exacerbates the anticompetitive effects of a regulatory decision, NYNEX and Rambus appear to condone a new and insidious form of implicit antitrust deference to regulation, one in which antitrust law must ignore conduct that exacerbates competitive harm because the company causing that harm wouldn’t have been in a position to do so but for regulation.151

Whatever one’s views of the substantive antitrust issues, the existence of antitrust injury is an antitrust question that should be decided by antitrust courts, and will not (and often cannot) be adequately addressed by regulatory agencies. And neither NYNEX nor Rambus discredits the notion that abuse of standard-setting processes can, in some circumstances, violate the antitrust laws. In particular, if the facts show that an agency relied upon misrepresentations in choosing a standard – and would have chosen a different standard but for the misrepresentations – then the defendant has caused a structural harm in the market even in the narrow Rambus view. In these circumstances, the defendant’s misrepresentations are the “but-for” cause of the defendant’s economic monopoly.152 While the D.C. Circuit refused to speculate on whether even this could constitute antitrust injury,153 it strains credulity to imagine any other outcome.

Like product-hopping, then, abuse of government standard-setting processes can cause competitive harm in markets. And like product-hopping, the harm may not be remediable through administrative recourse. The capture of government standard-setting processes offers yet another example of regulatory gaming, and another reason that antitrust courts should continue to play a role in regulated markets.

#### 4---deterrence---regulations don’t deter misconduct.

Dogan 08, \*Stacey L. Dogan, Professor of Law, Northeastern University; \*Mark Lemley, William H. Neukom Professor, Stanford Law School; of counsel, Keker & Van Nest LLP; (October 2008, “Antitrust Law and Regulatory Gaming”, https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1873&context=faculty\_scholarship)

Our goal in this paper is not to persuade the reader that these particular examples of regulatory gaming violate the antitrust laws (though we think they do) or that other examples, such as regulatory price squeezes, do not violate the antitrust laws. Rather, our point is that whether or not particular acts of regulatory gaming harm competition is and should be an antitrust question, not merely one that involves interpreting statutes or agency regulations. Regulatory agencies and even Congress cannot prevent gaming ex ante. Experience with the pharmaceutical industry suggests that if Congress acts to squelch one form of gaming, companies will find other ways to game the system. And even if Congress or the regulating body can surgically fix a particular type of exclusionary behavior, such an ex post response (unlike the threat of antitrust treble damages) does nothing to compensate for past harm or to deter future gaming behavior. Some level of antitrust enforcement – with appropriate deference to firm decisions about product design and affirmative regulatory decisions that affect market conditions – provides a necessary check on behavior, such as product hopping, that has no purpose but to exclude competition.

## CP — Advantage

#### Entanglement makes isolation impossible.

Acton 20, \*James M. Acton holds the Jessica T. Mathews Chair and is Co-Director of the Nuclear Policy Program at the Carnegie Endowment for International Peace. (March 23rd, 2020, “Cyber Warfare & Inadvertent Escalation.” Daedalus, vol. 149, no. 2, MIT Press, pp. 133–149)

There could be collateral effects even if a state’s networks for nuclear operations were entirely isolated; air-gapping (physically isolating one particular net- work from others) is, after all, not a cyber security panacea.30 Moreover, achieving perfect isolation could prove difficult in practice.31 To give but one reason, every nuclear-armed state, apart from the United Kingdom, has dual-use delivery systems, which can be used to deliver nuclear or non-nuclear weapons. Such delivery systems represent a potential point of contact between the C3I systems supporting nuclear operations and those supporting non-nuclear operations.

In practice, some nuclear-armed states–perhaps many or even all of them– have not tried to isolate their nuclear C3I systems. The United States, for example, has a number of dual-use C3I assets for communications and early warning that support both nuclear and non-nuclear operations.32 Other nuclear-armed states, including China and Russia, may as well, but are less transparent.33 Because the networks supporting dual-use C3I assets are likely to be connected directly to others involved in non-nuclear operations, there may be a particularly high risk of their being subject to collateral effects.

#### Federal oversight fails---litany of warrants.

Haber et al. 17, \*Eldar Haber, Senior Lecturer, University of Haifa, Faculty of Law; Haifa Center for Law and Technology, University of Haifa, Faculty of Law; Faculty Associate, Berkman-Klein Center for Internet & Society, Harvard University; \*\*Tal Zarsky, Vice Dean and Professor, University of Haifa, Faculty of Law; Haifa Center for Law and Technology, University of Haifa, Faculty of Law. (Winter 2017, “Cybersecurity for Infrastructure: A Critical Analysis”, https://ir.law.fsu.edu/cgi/viewcontent.cgi?article=2578&context=lr)

Ex-Ante Regulation and Optimizing Knowledge

The noted advantages of direct regulation of CI cyber risks seem to resolve many of the concerns noted in previous Sections. Yet, with these advantages come other problems. And while the global trend may be toward state-centric protection of CIs, many scholars and policymakers argue that this regulatory trajectory is unwise. Some find the claim that a single government entity “can micro-manage every aspect of cybersecurity and dictate best practice[s] is hubris.”210

One powerful set of critiques points to the inefficiency of the government-led regulatory scheme. These critiques state that government entities are not the optimal custodian and aggregator of knowledge in a cyber context.211 Quite to the contrary, it is more likely that knowledge generated and held by the state will prove to be subpar.212 Intuitively, in technological contexts, expertise lies mainly with external and diverse experts rather than the central government. The state can hire experts and learn from them, but so can private companies. There are no guarantees that the state will know which experts to listen to. Indeed, the state might be highly motivated to objectively choose the best solutions (we reconsider this notion below),213 but its lack of expertise could affect its choice and lead it to select a suboptimal strategy.

Beyond this general concern with the government’s inability to obtain relevant knowledge, we critically assess five specific shortcomings that pertain to various technological aspects of the cyber protection con- text. First, scholars opine that the negative impact of a government-led regulatory model could extend well beyond the level of CI protection re- quired, and affect aspects of cyber research. When the state, rather than the market, dictates conduct, this might affect overall innovation in the field.214 Innovation will be steered toward the specific issues government deems interesting, rather than naturally developing in an optimal direction. But an important caveat is due. Cyberspace is developing rap- idly; state influence may be minor and narrowly focused. Thus, innovation could proceed without substantial interference.

Second, even if the state were capable of establishing a reasonable blueprint to respond to cyber threats, it would have more difficulty in updating and amending this blueprint due to the fast pace of the constant, overall changes in the cyber field.215 The realm of cyber risks is highly volatile, and quick responses are necessary. In other fields, the fact that policy changes take time might not lead to devastating outcomes. It might even enable better policymaking, as it allows for re- sponsible decision making after in-depth consultation. This is not true for the cyber realm, which is arguably unique in that it is constantly undergoing change.216 For example, a powerful critique of the FERC standard-setting process in the energy market featured a slow-moving process, in which an updated standard was retracted at the time of its approval because it was already outdated.217

Third, state monitoring and enforcement could lead to an undesirable practice of ‘box checking’ or ‘box ticking.’218 When responsibility rests on the shoulders of the state to set standards for cyber defense, some corporations will simply comply without further examining whether such protection is optimal. Therefore, greater involvement of relevant players in the process is necessary. Note that this critique also pertains to other instances in which the defense standard is set by external (even commercial) parties.

Fourth, recent trends in the technological practices of private companies tend to further minimize the benefits of governmental regulation. In the past, such companies, including private CIs, relied upon proprietary software—computer code written specifically for them. However, financial and compatibility concerns pressured many companies to switch to Commercial, Off-The-Shelf (COTS) software.219 This transition offers advantages and disadvantages for cybersecurity that are beyond the scope of our analysis.220 However, this change has clear implications for our current discussion; with COTS, specific governments have less of an advantage in identifying and resolving cyber threats. Here, the global commercial market is faced with similar challenges, and it is likely that expertise lies there.

Finally, and perhaps most importantly, the state-driven and mandated mechanism of CI cyber defense is only meaningful when coupled with effective enforcement. Arguably, the state could impose various sanctions against companies that fail to comply, including requiring that they cease operations (note the authority vested with the DHS in the chemical sector), or terminating their CI license.221 However, enforcement is not easily achieved since it requires substantial resources. The FERC’s experiences in enforcing cyber defense standards illuminate the difficulties in enforcing such standards with government- budgeted manpower and resources.222 Furthermore, in many cases, private CIs that are subject to regulation are powerful entities that are not easily penalized by the regulator (certainly not severely—after all, they control a critical infrastructure). Notably, even without enforcement, a government-based approach could increase knowledge and im- prove information sharing in real time, but such goals could be achieved while applying more lenient, and even optimal, measures.

## DA — Gangster Antitrust

## DA — Interest Rates

#### Apple case thumps---it’s politicized, and has ripple effects across antitrust.

Albertgotti 9/10/21, \*[Reed Albergotti](https://www.washingtonpost.com/people/reed-albergotti/), Washington Post; (September 10th, 2021, “Judge’s ruling may take a bite out of Apple’s App Store, but falls short of calling the iPhone maker a monopolist”, https://www.washingtonpost.com/technology/2021/09/10/apple-epic-decision-judge-market-monopoly/)

A federal judge fundamentally altered Apple’s App Store business model on Friday in a landmark ruling that accused the iPhone maker of illegal anticompetitive behavior and is likely to have ripple effects across the U.S. antitrust landscape.

In a decision on an antitrust lawsuit brought by Fortnite maker Epic Games, U.S. District Judge Yvonne Gonzalez Rogers ruled that Apple must allow app developers to “steer” customers to alternatives to the tech giant’s payment processing service, which collects a 30 percent fee on most digital transactions. That was previously not allowed by the company, and marks a major victory for developers which have long complained of the tight grip the tech giant holds over its App Store on the roughly one billion iPhones currently in use.

[The blockbuster trial between Apple and the maker of ‘Fortnite’ goes out with a ‘hot tub’ session](https://www.washingtonpost.com/technology/2021/05/24/apple-epic-trial-hot-tubbing/?itid=lk_interstitial_manual_5)

Gonzalez Rogers also found that Apple was in violation of California state competition laws because of the way it forces developers into using Apple’s payment processing service without allowing them to tell customers there are alternatives, which are often cheaper.

She stopped short of ruling in favor of Epic‘s claims that Apple is a monopolist, although she left the door open by suggesting more evidence could have changed her decision.

“The court does not find that it is impossible; only that Epic Games failed in its burden to demonstrate Apple is an illegal monopolist,” she wrote.

Epic spokeswoman Elka Looks said the company plans to appeal the ruling. Tim Sweeney, chief executive of Epic, said in a tweet that, “Today’s ruling isn’t a win for developers or for consumers.”

Apple did not respond to requests for comment.

The ruling, one of the first major legal actions taken against a tech giant in a new era of antitrust scrutiny, is sure to echo loudly both in Washington, where a legislative effort to rein in the power of Big Tech is underway, and in the courts, which are facing the biggest test of existing antitrust laws in decades. Tech giants have come under the microscope in recent years as it became clear that current antitrust law does not effectively address their power, and regulators and lawmakers have been pushing to change that.

#### Biden executive order outweighs.

Posner 21, professor at the University of Chicago Law School (Eric, 7-21-2021, "The Antitrust War’s Opening Salvo", Project Syndicate, <https://www.project-syndicate.org/commentary/biden-antitrust-executive-order-what-it-does-by-eric-posner-2021-07>)

CHICAGO – US President Joe Biden’s new executive order on “Promoting Competition in the American Economy” is more significant for what it says than for what it does. In fact, the order doesn’t actually order anything. Rather, it “encourages” federal agencies with authority over market competition to use their existing legal powers to do something about the growing problem of monopoly and cartelization in the United States. In some cases, the relevant agencies are asked merely to “consider” ramping up enforcement; in others, they are directed to issue regulations, but the content of those regulations remains largely up to them.

Nonetheless, it would be a mistake to dismiss the order’s tentative language as mere rhetoric. Antitrust is the main body of law governing market competition in the US, and it has been the object of sustained attack by business interests and conservative intellectuals for more than 50 years. Biden is the first president since Harry Truman to take a strong public [anti-monopoly stand](https://www.project-syndicate.org/commentary/new-brandeisians-antitrust-for-big-tech-by-eric-posner-2021-06), and he has backed it up by [appointing](https://www.politico.com/news/2021/07/20/biden-picks-doj-antitrust-chief-500310) ardent anti-monopoly advocates to his government.

The executive order is ambitious in its scope and style. In strongly worded passages, it accuses businesses of monopolistic and unfair practices in major industries, including technology, agriculture, health care, and telecommunications. It laments the decline of government antitrust enforcement, and identifies numerous harms that have resulted – including economic stagnation and rising inequality.

The order also establishes a new bureaucratic organization in the White House to lead the anti-monopoly effort. Demanding a “whole-of-government” approach, it calls on the vast resources of numerous agencies, and not just the two that traditionally oversee antitrust (the Department of Justice and the Federal Trade Commission).

#### Interest rate hikes are bad — they undermine the stock market and decimate businesses

O’Connell & Curry 21 — Brian O’Connell & Benjamin Curry; “What Happens When the Fed Raises Interest Rates?;” Forbes; June 18th, 2021; https://www.forbes.com/advisor/investing/fed-raises-interest-rates/

When the Fed raises the federal funds target rate, the goal is to increase the cost of credit throughout the economy. Higher interest rates make loans more expensive for both businesses and consumers, and everyone ends up spending more on interest payments.

Those who can’t or don’t want to afford the higher payments postpone projects that involve financing. It simultaneously encourages people to save money to earn higher interest payments. This reduces the supply of money in circulation, which tends to lower [inflation](https://www.forbes.com/advisor/investing/what-is-inflation/) and moderate economic activity—a.k.a. cool off the economy.

Let’s look at how this applies to a 1% increase in the fed funds rate and how that might impact the lifetime cost of a [home mortgage loan.](https://www.forbes.com/advisor/mortgages/how-the-fed-affects-mortgage-rates/) Take a family shopping around for a $300,000 30-year, fixed-rate mortgage. If banks were offering them an interest rate of 3.5%, the total lifetime cost of the mortgage would be approximately $485,000, with nearly $185,000 of that accounting for interest charges. Monthly payments would clock in around $1,340. Let’s say the Fed had raised interest rates by 1% before the family got a loan, and the interest rate offered by banks for a $300,000 home mortgage loan rose to 4.5%. Over the 30-year life of the loan, the family would pay a total of more than $547,000, with interest charges accounting for $247,000 of that amount. Their monthly mortgage payment would be approximately $1,520. In response to this increase, the family in this example might delay purchasing a home, or opt for one that requires a smaller mortgage, to minimize the size of their monthly payment. This (very) simplified example shows how the Fed reduces the amount of money in the economy when it raises rates. Besides mortgages, rising interest rates impact the stock and bond markets, credit cards, personal loans, student loans, auto loans and business loans.

Impact on Stocks

Higher market interest rates can have a negative impact on the [stock market](https://www.forbes.com/advisor/investing/what-is-the-stock-market/). When Fed rate hikes make borrowing money more expensive, the cost of doing business rises for public (and private) companies. Over time, higher costs and less business could mean lower revenues and earnings for public firms, potentially impacting their growth rate and their stock values.

“If the cost of borrowing money from a bank increases, the opportunity to expand investment in capital goods by a corporation stalls,” says Dan Chan, a Silicon Valley investor and a former pre-IPO employee of PayPal. “The interest rate may be so high that many companies will not be able to afford to grow.”

More immediate is the impact Fed rate increases have on market psychology, or how investors feel about market conditions. When the FOMC announces a rate hike, traders might quickly sell off stocks and move into more defensive investments, without waiting for the long, complicated process of higher interest rates to work their way through the entire economy.

# 1AR

## Adv — Innovation

#### Insecurity is baked in---appeasing China fails, the best option now is deterrence.

Small et al. 20, \*Andrew Small is a senior transatlantic fellow with the Asia program at the German Marshall Fund of the United States and an associate senior policy fellow at the European Council on Foreign Relations. He previously worked as the director of the Foreign Policy Centre’s Beijing office and was a visiting fellow at the Chinese Academy of Social Sciences; \*Dhruva Jaishankar is director of the U.S. Initiative at the Observer Research Foundation (ORF) and a non-resident fellow at the Lowy Institute in Australia. He previously worked at Brookings India, the German Marshall Fund, and the Brookings Institution; (July 2020, ““For Our Enemies, We Have Shotguns”: Explaining China’s New Assertiveness”, https://warontherocks.com/2020/07/for-our-enemies-we-have-shotguns-explaining-chinas-new-assertiveness/)

Yet many of the decisions facing these countries also involve calculations about immediate issues with China — border incursions, threats of economic punishment, Hong Kong’s status — that hinge more directly on the nature of the Chinese leadership’s current outlook. If Beijing is in an insecure, defensive mode, one argument would be that the best course of action is to find ways to ease tensions. But this would evidently be the worst path to pursue if other explanations of its behavior hold true, either confirming for China the most hubristic assessment of its own position or encouraging even bolder acts of adventurism. It would also do little good if Beijing’s insecurity has already led it to conclude that it is now in an all-out struggle.

The alternative hypothesis — that carefully treading around the Chinese government’s sensitivities during a period in which it faces intense pressure will elicit a cooler-headed approach — has also been [tested out](https://www.theatlantic.com/ideas/archive/2020/05/how-should-biden-handle-china/612052/) to bruising effect. Indeed, previous governments in [the United States](https://www.brookings.edu/blog/up-front/2013/06/10/obama-and-xi-at-sunnylands-a-good-start/), [India](https://www.tandfonline.com/doi/abs/10.1080/0163660X.2019.1592364), and [Japan](https://www.tandfonline.com/doi/abs/10.1080/00927678.2012.678130) attempted to play down differences to no avail. More recently, the [shock in Europe](https://www.ecfr.eu/publications/summary/the_meaning_of_systemic_rivalry_europe_and_china_beyond_the_pandemic) over China’s behavior resulted not just from Beijing’s actions, but from the fact that they followed precisely such an effort on the part of European leaders to provide [discreet support](https://www.politico.eu/interactive/inside-emmanuel-macron-coronavirus-war/) [to China](https://www.euractiv.com/section/eu-china/news/no-progress-on-trade-investment-hong-kong-as-eu-wraps-up-tense-china-summit/) at the peak of its internal crisis. This was met, in Gui’s words, with shotguns.

Demonstrating to China’s leadership that a wider de-escalation is preferable will instead require others to raise the costs of adverse Chinese behavior and signal further repercussions if Beijing continues down its current path. Initially this could range from symbolic moves, such as suspensions of high-level meetings with China and the launch of new processes among democracies openly focused on China policy coordination, to targeted measures against Chinese Communist Party officials, and a significant tightening of dual-use equipment sales. There is no guarantee that tougher measures will moderate Beijing’s approach — it is entirely possible that China is simply set on its new trajectory, thinking either that it will pay off in the end or that there is no alternative option. But the Chinese Communist Party has repeatedly shown the pragmatic capacity to correct course when absolutely necessary. This is the moment for collective efforts to sharpen that choice.

#### Maritime expansion proves revisionism

**Grady 19** – John; former managing editor of the Navy Times, retired as director of communication for the Association of the US Army. (“Chinaʻs Coast Guard Enforcing Its Blue Water Territorial Expansion” USNI News. Published 11/19/19, accessed 11/20/19. <https://news.usni.org/2019/11/19/chinas-coast-guard-enforcing-blue-its-intended-water-territorial-expansion>) //sjr

The rapid expansion of China’s Coast Guard gives Beijing the means to shift its sea expansion aims from aspirational to operational, a panel of security experts concurred during a Monday event detailing China’s maritime ambitions. In vast stretches of sea, an area stretching from the Senkaku Islands in the East China Sea to the Scarborough Shoals off the Phillippines in the South China Sea, China’s maritime forces are aggressively asserting claims to every landmass — natural or manmade — in this blue territory, the experts from several think tanks agreed while speaking at the Center for Strategic and International Studies. During the past few years, China’s Coast Guard increased the number of its intrusions into the waters around the uninhabited islands dotting the East China Sea that are also claimed by Taiwan, said Masahi Murano, a fellow at the Hudson Institute. The increase, Murano added, is, “because they are rapidly building Coast Guard vessels.” China has more than doubled the number of ships in this fleet. The People’s Liberation Army Navy controls 135 coast guard ships, translating into an increased frequency of intrusions — from three to now four times monthly — with larger, more heavily armed vessels to press China’s claims, Murano said. Japan’s 62 coast guard vessels capable of sustained at-sea operations “are not really in position to shape Chinese actions” in the East China Sea, added Jeffrey Hornung, a political scientist at the RAND Corporation. “Our resources are not unlimited” in finances or manpower to compete with Beijing vessel for vessel and crew for crew, Murano said. An additional limitation is Japan’s Coast Guard is a purely constabulary force. Hornung agreed, suggesting Japan should focus investments in intelligence, surveillance and reconnaissance assets to deter and counter Chinese ambitions. Questioning Tokyo’s decision to re-purpose two destroyers partially in answer to China’s announced goal of having six aircraft carriers by 2030, Murano said, “Carriers are not the wave of the future,” Murano said Beijing’s objective with such gray zone challenges as sending vessels to intrude into the area sending land-based aircraft on flyover missions, is to cause regional competitors to spend heavily on their defenses. Eventually, China aims to present Japan with a “fait accompli” in enforcing China’s claims to the islands, Murano said. Further south, in the South China Sea, Beijing’s maritime ambitions are similarly presenting grey zone challenges to an American treaty ally — the Philippines. The country’s leadership “doesn’t know if it can rely on the United States” in its dispute with China over Scarborough Shoals, said Greg Poling, director of CSIS’ Asia Maritime Transparency Initiative. Philippine President Rodrigo Duterte has questioned American resolve, at a time when an international tribunal determined in 2016 that the shoals, about 120 miles from Subic Bay, [were Philippine territory](https://news.usni.org/2019/08/15/philippines-pushing-back-against-chinese-militia-south-china-sea-presence), Poling said. However, since the ruling, Hornung said the dynamics in the South China Sea have changed dramatically. The Chinese have transitioned from turning coral reefs into islands to having them become effectively homeports for Chinese Coast Guard vessels and forward landing bases for maritime patrol aircraft. They have also installed sophisticated mobile air and maritime defense systems as well as jamming equipment on them. In addition to a permanent coast guard and air presence, “300 naval militia vessels are operating every day” in the South China Sea, Hornung said. They use manmade islands as home ports to send ships out to contest Vietnam’s claims to seabeds holding energy resources and minerals and contest Phillippine fishing rights to work waters in its economic zone. The objective in all this activity is “to make it politically risky” for “civilians to operate in their own EZ’s,” he added. “Beijing wants to shape our behavior,” Collin Koh Swee Lean, a research fellow at Nanyang Technological University in Singapore, said. “What we are seeing up is the beefing up of these outposts and [their long-term] maintenance.” He added that attention to long-term detail comes down to Chinese engineers studying the impact of the bonding or coral and concrete to ensure these bases remain in place rather than sink into the sea or have them corrode out of existence. Long-term, China’s aims appear to involve much more than expanding maritime or territorial claims. The Chinese are pursuing “underwater observations, acoustics,” areas of importance over the next five to 10 years economically and militarily, Lean said. Deterring China in the East China Sea needs to involve strengthening security ties between Japan, the United States and other regional powers such as Australia and India, Murano and Hornung said. In the case of reassuring the Philippines of America’s continued commitment to its defense, Hornung said recent exercises between the two nations was a positive step. Still, they need to be expanded and made regular.

#### China plans to export its domestic authoritarianism globally.

McMaster 20, \*H.R. McMaster, Fouad and Michelle Ajami Senior Fellow at the Hoover Institution, Stanford University. (May 2020, “How China Sees the World”, https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/)

As China pursues its strategy of co-option, coercion, and concealment, its authoritarian interventions have become ubiquitous. Inside China, the party’s tolerance for free expression and dissent is minimal, to put it mildly. The repressive and manipulative policies in Tibet, with its Buddhist majority, are well known. The Catholic Church and, in particular, the fast-growing Protestant religions are of deep concern to Xi and the party. Protestant Churches have proved difficult to control, because of their diversity and decentralization, and the party has forcefully removed crosses from the tops of church buildings and even demolished some buildings to set an example. Last year, Beijing’s effort to tighten its grip on Hong Kong sparked sustained protests that continued into 2020—protests that Chinese leaders blamed on foreigners, as they typically do. In Xinjiang, in northwestern China, where ethnic Uighurs mainly practice Islam, the party has forced at least 1 million people into concentration camps. (The government denies this, but last year The New York Times uncovered a cache of incriminating documents, including accounts of closed-door speeches by Xi directing officials to show “absolutely no mercy.”)

Party leaders have accelerated the construction of an unprecedented surveillance state. For the 1.4 billion Chinese people, government propaganda on television and elsewhere is a seamless part of everyday life. Universities have cracked down on teaching that explains “Western liberal” concepts of individual rights, freedom of expression, representative government, and the rule of law. Students in universities and high schools must take lessons in “Xi Jinping Thought on Socialism With Chinese Characteristics for a New Era.” The chairman’s 14-point philosophy is the subject of the most popular app in China, which requires users to sign in with their cellphone number and real name before they can earn study points by reading articles, writing comments, and taking multiple-choice tests. A system of personal “social credit scores” is based on tracking people’s online and other activity to determine their friendliness to Chinese government priorities. Peoples’ scores determine eligibility for loans, government employment, housing, transportation benefits, and more.

The party’s efforts to exert control inside China are far better known than its parallel efforts beyond China’s borders. Here again, insecurity and ambition are mutually reinforcing. Chinese leaders aim to put in place a modern-day version of the tributary system that Chinese emperors used to establish authority over vassal states. Under that system, kingdoms could trade and enjoy peace with the Chinese empire in return for submission. Chinese leaders are not shy about asserting this ambition. In 2010, China’s foreign minister matter-of-factly told his counterparts at a meeting of the Association of Southeast Asian Nations: “China is a big country, and you are small countries.” China intends to establish a new tributary system through a massive effort organized under three overlapping policies, carrying the names “Made in China 2025,” “Belt and Road Initiative,” and “Military-Civil Fusion.”

#### China won’t succumb to the international order.

McMaster 20, \*H.R. McMaster, Fouad and Michelle Ajami Senior Fellow at the Hoover Institution, Stanford University. (May 2020, “How China Sees the World”, https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/)

The Chinese Communist Party is not going to liberalize its economy or its form of government. It is not going to play by commonly accepted international rules—rather, it will attempt to undermine and eventually replace them with rules more sympathetic to China’s interests. China will continue to combine its form of economic aggression, including unfair trade practices, with a sustained campaign of industrial espionage. In terms of projecting power, China will continue to seek control of strategic geographic locations and establish exclusionary areas of primacy.

Any strategy to reduce the threat of China’s aggressive policies must be based on a realistic appraisal of how much leverage the United States and other outside powers have on the internal evolution of China. The influence of those outside powers has structural limits, because the party will not abandon practices it deems crucial to maintaining control. But we do have important tools, quite apart from military power and trade policy.

For one thing, those “Western liberal” qualities that the Chinese see as weaknesses are actually strengths. The free exchange of information and ideas is an extraordinary competitive advantage, a great engine of innovation and prosperity. (One reason Taiwan is seen as such a threat to the People’s Republic is because it provides a small-scale yet powerful example of a successful political and economic system that is free and open rather than autocratic and closed.) Freedom of the press and freedom of expression, combined with robust application of the rule of law, have exposed China’s predatory business tactics in country after country—and shown China to be an untrustworthy partner. Diversity and tolerance in free and open societies can be unruly, but they reflect our most basic human aspirations—and they make practical sense too. Many Chinese Americans who remained in the United States after the Tiananmen Square massacre were at the forefront of innovation in Silicon Valley.

#### Pushback is key to undermine support for their model.

McMaster 20, \*H.R. McMaster, Fouad and Michelle Ajami Senior Fellow at the Hoover Institution, Stanford University. (May 2020, “How China Sees the World”, https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/)

Without effective pushback from the United States and like-minded nations, China will become even more aggressive in promoting its statist economy and authoritarian political model. For me, the state visit to Beijing—and exposure to China’s powerful combination of insecurity and ambition—reinforced my belief that the United States and other nations must no longer adhere to a view of China based mainly on Western aspirations. If we compete aggressively, we have reason for confidence. China’s behavior is galvanizing opposition among countries that do not want to be vassal states. Internally, the tightening of control is also eliciting opposition. The bravado of Li Keqiang and other officials may be intended to evoke the idea of China as sovereign of “everything beneath heaven,” but many beneath heaven do not, and must not, agree.