# 1AC

## 1AC

### Plan

#### Plan: The United States federal government 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---Innovation ADV

#### Advantage 1 is Innovation:

#### Current standard setting organization and FRAND enforcement is failing now

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.

#### Holdup is accentuated by FTC v Qualcomm

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

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.

#### Holdup threatens the entire IOT economy.

Morton 16, \*Fiona M. Scott Morton is an American economist, currently the Theodore Nierenberg Professor at Yale School of Management; \*Carl Shapiro is the Transamerica Professor of Business Strategy at the Haas School of Business at the University of California at Berkeley; (2016, “Patent Assertions: Are We Any Closer to Aligning Reward to Contribution?”, https://www.journals.uchicago.edu/doi/full/10.1086/684987#\_i22)

G. Summary

However, our overall conclusions regarding SEPs are more mixed. Policy and legal changes that have reduced the ability of SEP owners to engage in patent holdup appear to have stalled out, especially as regards reform of the IPR rules at SSOs other than the IEEE. If so, this could have important effects on innovation and efficiency. For example, the “Internet of Things” is a new and growing area where royalty stacking and patent holdup appear to be very real dangers. Devices of all sorts, from thermostats to railroad cars to refrigerators, are being given connectivity using standards developed by SSOs. The price of those chips, and whether the IP contained in them costs $5 or $0.50 or $0.005, will determine the nature of new applications and the rate of adoption.

Failure to prevent patent holdup relating to tomorrow’s information technology and communications standards is likely to cause significant social welfare loss in the years ahead. If new and more effective private solutions relating to standard setting do not emerge to promote innovation and protect consumers, antitrust enforcement is one of the only remaining remedies that seems feasible.

V. Conclusions

Over the past five years, the rewards provided to patent owners in the United States have become more closely matched with the value of the technology they contribute. When rewards and contributions are aligned, economic efficiency is promoted because investments into developing new technologies are commensurate with benefits. These changes have come from legislation, the federal courts, and policy statements and enforcement actions by regulators of various types. However, at this juncture, we see a substantial gap persisting between the ability of some patent owners to monetize their patents and the contributions provided by the technology underlying those patents. With the “Internet of Things” poised to create economic growth, this is a problem worthy of further research and policy attention.

#### 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.

#### Patent holdup is real and necessitates intervention, even if it can’t be systemically proven.

Contreras 19, \*Jorge Contreras, Professor, University of Utah S.J. Quinney College of Law; (2019, “MUCH ADO ABOUT HOLD-UP”, <https://www.illinoislawreview.org/wp-content/uploads/2019/08/Contreras.pdf>)

B. Protective Measures May Already Be Working to Reduce Hold-Up

Another important factor that should be considered regarding the purported lack of empirical evidence of systemic hold-up is the effect that existing policy measures have already had in reducing hold-up. As noted above, the threat of patent hold-up was a primary motivating factor for many SDOs to adopt policies requiring the disclosure and licensing of SEPs. These policies have been in place for decades. In the United States, the first such policy was adopted in 1959 by the American Standards Association (the predecessor to today’s American National Standards Institute (ANSI).102 Today, every one of the more than 200 ANSI-accredited developers of American National Standards must adhere to ANSI’s essential requirements, including the adoption of such a licensing policy for SEPs. Similar policies have existed in European and international standards organizations since at least the 1980s.103 These policies, which were developed by SDOs in large part to reduce the likelihood of hold-up within standard-setting systems, have had several decades to work, and it is likely that the lack of observed hold-up in some studies can be attributed to the successful operation of these policies.

Similarly, antitrust and competition enforcement agencies in the U.S. and Europe have been aware of the potential for hold-up connected with standardization for many years. Accordingly, they have brought enforcement actions when it has been alleged that hold-up behavior has resulted in a violation of the antitrust laws. High-profile enforcement actions against patent holders such as Rambus, 104 Google 105 and Qualcomm106 send powerful deterrent signals to the market and warn others not to engage in similar behavior lest they, too, become the subject of agency enforcement. Like SDO policies, it is likely that the general market awareness of agency interest in standard-setting and hold-up has, to a degree, limited the amount of hold-up that is actually attempted in the marketplace, thereby limiting the direct evidence of hold-up as a systemic problem.

But do the deterrent effects of SDO and agency efforts to reduce hold-up signify that hold-up is not a problem? Certainly not. To reach such a conclusion would be perverse: akin to claiming that burglary is not a problem in a neighborhood that experiences reduced burglary rates after it has implemented an active neighborhood watch program and enhanced policing.

C. Indicia of Healthy Markets do not Prove the Absence of Anticompetitive Conduct

As noted above, one of the principal arguments advanced by commentators seeking to refute the “hold-up theory” is that markets for telecommunications products, namely smart phones, are robust – evidenced by increasing product functionality, decreasing consumer prices and rapid innovation -- and that this degree of robustness indicates that hold-up cannot be a problem in these markets.107 If hold-up were a problem in these markets, they reason, we would see product stagnation, stable (but high) prices, and a lack of competition – features associated with classic examples of hold-up in markets for products such as natural resources and agricultural goods.108

But this argument relies on a false syllogism: hold-up results in market dysfunction; if a market functions well, then it cannot be subject to hold-up. The weaknesses in this argument are multifold. First, hold-up may exist in individual instances without sufficient weight to affect overall market characteristics, particularly in a large global market such as mobile telecommunications. Thus hold-up may exist, even in a market that outwardly appears to be functioning well. Second, there is no valid counterfactual to use to compare the health and robustness of the market for mobile telecommunications products.109 Other consumer electronics devices, such as televisions and DVD players, do not compare well with mobile telecommunications devices, which have taken on a unique character in the modern networked economy. Thus, observing the strength of the market fails to answer the critical questions “compared to what?” and how much stronger the market might be (through more product diversity, functionality, price reduction) without hold-up?

A simple historical illustration is useful in this context. During the decade leading up to the enactment of the Sherman Antitrust Act of 1890, several major U.S. commodity markets (e.g., steel, salt, petroleum, coal, sugar, lead, and others) came under intense scrutiny for a variety of allegedly anticompetitive industrial arrangements. One might have argued that these markets, had they been subject to the sorts of anticompetitive collusion that the Sherman Act sought to address, should have seen reductions of output and increases in price. Yet, between 1880 and 1890, U.S. output of salt, petroleum, steel, and coal all increased significantly, and prices of steel, sugar and lead all dropped significantly.110 Do these positive market indicia demonstrate that the subject markets were not subject to anticompetitive collusion, and that the Sherman Act was not necessary? Certainly, investigations of these industries revealed significant cartel behavior. I would suggest that few commentators today would argue that the coal, steel, sugar and other major industrial producers of the late nineteenth century were innocent of collusive and anticompetitive conduct, or that the Sherman Act was not a necessary and beneficial measure for the U.S. economy.111 Yet, had we relied solely on the positive characteristics exhibited by these markets as proof that anticompetitive conduct did not exist, then perhaps the Sherman Act never would have been enacted.

By the same token, the fact that global markets for standardized products such as computers and smart phones appear to be thriving does not itself refute the possibility of hold-up nor the existence of anticompetitive conduct in these markets. Nor does it allow regulators and policy makers to drop their guard or cease to monitor these important industries.

#### The plan requires SSO’s to administer reasonable action to prohibit ex post opportunism---that solves

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.

### 1AC---Cybersecurity ADV

#### 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.

#### 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.

# 2AC

## K

### 2AC- 6

#### There are countless examples of Black women’s efforts in the labor movement successfully materializing change.

Kelly 19, \*Kim Kelly is a freelance journalist and organizer based in Philadelphia. Her work on labor, class, politics, and culture has appeared in the New Republic, the Washington Post, the Baffler, and Esquire, among other publications, and she is the author of FIGHT LIKE HELL, a forthcoming book of intersectional labor history. (February 23rd, 2019, “Black Women in the Labor Movement Have Long Defended American Workers”, https://www.teenvogue.com/story/black-women-in-the-labor-movement)

Black leaders, activists, and organizers formed the backbone of the U.S. labor movement. Even when the forces of structural racism and segregation sought to stifle their contributions, their resolve to fight for workers’ rights alongside the cause of civil rights remained unshakable. Black women, in particular, have played an enormous role in the movement’s legacy and development.

The Washerwomen of Jackson formed Mississippi’s first labor union in 1866. Lucy Parsons, the anarchist firebrand, cofounded three influential radical unions in 20th-century Chicago. More recently, United Auto Workers (UAW) organizer Sanchioni Butler [battled](https://ips-dc.org/black-workers-are-organizing-at-nissan/) Nissan in a years-long campaign to organize Southern auto-plant workers. Along with so many others, these Black women have long been the bedrock of a workers’ rights movement that has often tried to shut them out.

Prior to desegregation, many white-led unions [refused](https://www.teenvogue.com/story/black-activists-shaped-the-labor-movement) to admit Black members of any gender, and Black women faced the intersectional double bind of gender bias and racial discrimination. When faced with a locked union hall door, however, many Black women labor leaders decided to take matters into their own hands and formed their own organizations within the industries in which they had the highest numbers and therefore held the most power.

In 1866, a group of newly emancipated Black women working as laundresses in Jackson, Mississippi, [formed](http://www.seiu-uhw.org/archives/20663) the state’s first labor union by sending a [resolution](http://www.sojournertruth.net/mississippisfirst.pdf) to the mayor, informing him that they would henceforth be charging a “uniform rate” for their labor. Two decades later, in Atlanta, [98% of Black working women](https://progressive.org/dispatches/we-mean-business-or-no-washing-atlanta-washerwomen-strike_180205/) in the city were employed as domestic workers, and those who worked long, back-breaking hours as laundresses organized the Atlanta Washerwomen's Strike, demanding fixed wages. Their numbers grew from 20 to 3,000 people, and they also invited white laundresses to join them in a show of interracial solidarity that was nearly unheard of at the time.

The examples of Southern Black women organizers continue with leaders including Sylvia Woods, a New Orleans–born laundry worker–turned–union activist who in Chicago participated in one of the first sit-down strikes of the Depression era; Rosina Tucker, who helped organize the first AFL-CIO–recognized Black labor union and helped [organize laundry workers, domestic workers, and hotel and restaurant workers](https://timeline.com/rosina-tucker-pullman-porters-37ba63c2b9eb), jobs that at the time were primarily held by Black women; and [Dorothy Lee Bolden](https://www.teenvogue.com/story/black-activists-shaped-the-labor-movement).

Bolden, who started working in domestic service at the age of 9 and [founded](http://aarlarchives.blogspot.com/2011/11/mrs-dorothy-lee-bolden-founder-and.html) the National Domestic Workers Union of America in [1968](https://blog.library.gsu.edu/2011/09/07/dorothy-bolden-gives-voice-to-atlanta%E2%80%99s-%E2%80%9Chelp%E2%80%9D/), was involved [in the fight for labor and civil rights](https://www.huffingtonpost.com/entry/stacey-abrams-georgia-domestic-workers_us_5bd8a9cbe4b0da7bfc14a210), and her organizing work within an often exploited industry made a [huge impact](http://aarlarchives.blogspot.com/2011/11/mrs-dorothy-lee-bolden-founder-and.html) on the lives of domestic workers, both in Atlanta and far beyond the city limits. Bolden is now hailed as an Atlanta labor icon, and, according to the Georgia State University library [website](https://blog.library.gsu.edu/2011/09/07/dorothy-bolden-gives-voice-to-atlanta%E2%80%99s-%E2%80%9Chelp%E2%80%9D/), at its height, the union she founded “claimed to represent 30,000 people and played a part in fundamentally changing the treatment of domestic workers under U.S. labor law.”

Their legacies continue through modern union organizers, including the UAW’s [Sanchioni Butler](https://and-still-i-rise.org/wp-content/uploads/2015/04/SanchoniButler.pdf), Communications Workers of America’s (CWA) [Sandra Joyce Bellamy](https://and-still-i-rise.org/wp-content/uploads/2015/04/SandraJoyce.pdf), and UNITE HERE’s [Wilna Destin](https://and-still-i-rise.org/wp-content/uploads/2015/04/WilnaDestin.pdf).

Butler, Bellamy, and Destin are all profiled alongside 24 other Black women labor leaders in the 2015 project [And Still I Rise: Black Women Labor Leaders’ Voices, Power and Promise](https://and-still-i-rise.org/about/), which was part of the Black Worker Initiative, from the Institute for Policy Studies. “We know that they are, and have always been, ‘the miner’s canary’ for workers in America. Black women have experienced for decades many of the economic and social ills now faced by others. Therefore, it stands to logic that making black women whole raises the floor for all women—likely, for all workers,” consultant Kimberly Freeman Brown and Marc Bayard, director of the Institute for Policy Studies' Black Worker Initiative, write in the project’s introduction.

Chicago and New York City — specifically Harlem — have long been hotbeds of Black labor activity, too. Harlem’s Dora Lee Jones helped establish the Domestic Workers' Union. Maida Springer Kemp, who was born in Panama and moved to Harlem as a child, was heavily involved in labor struggles. During the Depression, she worked in a garment factory and became [involved](https://www.post-gazette.com/news/obituaries/2005/03/31/Obituary-Maida-Springer-Kemp-Labor-activist-traveled-worldwide/stories/200503310254) in its union, the International Ladies' Garment Workers' Union (ILGWU), working her way up through various positions. She was also involved with labor organizing in Kenya, Ghana, and Tanzania, and was named the AFL–CIO's representative to Africa in 1959, making her the [first](http://www.seiu-uhw.org/archives/20663) Black woman to represent U.S. labor abroad.

Lucy Parsons was [born](https://www.chicagotribune.com/lifestyles/books/ct-books-lucy-parsons-goddess-of-anarchy-jacqueline-jones-20171108-story.html) into slavery in Virginia in 1853. After the Civil War ended and emancipation was declared, she moved to Texas, as a teenager, where she met her husband, Albert Parsons, a former Confederate soldier turned anarchist. They were forced to flee the state because of the [danger](https://www.iww.org/history/biography/LucyParsons/1) posed by those who opposed their interracial marriage, and they landed in Chicago in 1873. They [joined](https://ufcw324.org/lucy-parsons-the-timeless-rebel/) the Knights of Labor, and in 1883, they [founded](https://blavity.com/labor-day-labor-hero-lucy-parsons) the International Working People’s Association (IWPA); they both contributed articles to various anarchist and labor publications, and Lucy ran a dressmaking shop, where she held secret [meetings](https://www.iww.org/history/biography/LucyParsons/1) with other Chicago garment workers. In 1886, they led the city’s [first May Day parade](https://www.dnainfo.com/chicago/20170501/avondale/lucy-gonzalez-parsons-street-sign-avondale-may-day-1886-labor-organizer/), which came with a call for an eight-hour workday.

After Albert and three other anarchists were [unjustly](https://www.chicagotribune.com/news/ct-xpm-2004-05-13-0405130278-story.html) executed by the state following the notorious [Haymarket Affair](https://www.history.com/news/remembering-the-haymarket-riot), Lucy [dedicated](https://www.dnainfo.com/chicago/20170501/avondale/lucy-gonzalez-parsons-street-sign-avondale-may-day-1886-labor-organizer/) the rest of her life to fighting for the working class and for revolution.

In 1900, she was a key organizer for the newly founded [ILGWU](http://ilgwu.ilr.cornell.edu/history/), and five years later, she was a founding member of the more radical Industrial Workers of the World (IWW), which [welcomed](https://www.teenvogue.com/story/black-activists-shaped-the-labor-movement) women and Black workers. She also helped [organize](https://www.chicagotribune.com/news/ct-xpm-2004-05-13-0405130278-story.html) Chicago’s Working Women’s Union No. 1 (WWU), and in later years, she threw herself into the Communist Party’s International Labor Defense group. Due to Lucy's militancy, her powerful oratory skills, and her unwavering dedication to the cause, the [Chicago Police Department](https://blavity.com/labor-day-labor-hero-lucy-parsons) famously considered her to be “more dangerous than a thousand rioters.”

These are only a few examples of the amazing Black women labor leaders whose work has shaped the course of history. New leaders are being minted and elected every day. Take, for example, Minnesota Representative Ilhan Omar, who comes from a labor background and who [told](https://www.teenvogue.com/story/midterms-labor-candidates) Teen Vogue, “A better future can only be secured when there is a collective fight working toward a greater vision.”

Black women’s voices have been suppressed and left unrecognized for far too long, even within a workers’ rights movement that they helped build from the ground up. It’s vitally important to learn their history and support their modern-day counterparts’ work, because without Black women, the U.S. labor movement undoubtedly would have been doomed from the start.