# Round 5 wikidoc

# 1AC — SEP’s

## 1AC

### 1AC---FRAND ADV

#### Advantage 1 is FRAND:

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

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

I. Standard Setting and the Competitive Process

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

#### Monopoly pricing and selective licensing undermines 5G innovation---FRAND enforcement is key.

Actonline 20, the App Association represents more than 5,000 app companies and information technology firms across the mobile economy; (August 26th, 2020, “Save Our Standards: The Ninth Circuit Court of Appeals Reverses Decision in FTC v. Qualcomm”, <https://actonline.org/2020/08/26/save-our-standards-the-ninth-circuit-court-of-appeals-reverses-decision-in-ftc-v-qualcomm/>)

* Ability edited

Moreover, the FRAND agreement is a critical tool used by standard setting organizations to ensure the process enhances competition and does not run afoul of antitrust laws. Generally, a collaboration between competitors to choose market winners or set prices raises significant questions for competition regulators. Royalty free and FRAND licensing requirements were created by standards bodies to avoid potential antitrust scrutiny by limiting the market power and the potential for abuse by those involved in developing a standard. This is why the American National Standards Institute (ANSI) will not accredit any standards developing organization (SDO) that does not require standard-essential patent holders to provide licensing terms at least as favorable as FRAND.

The most important beneficiary of open interoperability standards and FRAND licensing requirements are the entrepreneurs and small businesses that have long fueled America’s innovation engine. They don’t have giant patent portfolios, market power, or the resources to hire legions of lawyers and spend years battling SEP abusers in civil court. Without some level of certainty about their ability to obtain licenses—let alone what they may cost—entrepreneurs will have trouble justifying the pursuit of any innovation that uses a standard and will certainly struggle to raise money from investors for such innovation. And Qualcomm’s vague and toothless promise simply “not to sue” smaller companies and component makers is no substitute for a license.

The adoption of 5G technology is expected to open unprecedented opportunities for innovation and economic growth as we move toward a world where everything from cars to tractors to buildings will connect to wireless networks. At every stage of the information technology revolution, America has been the undisputed leader because of the unparalleled entrepreneurial innovation ecosystem that we have built. If 5G SEP holders are able to arbitrarily refuse licenses to smaller firms, it would ~~cripple~~ undermine America’s innovation ecosystem at the start of the next big wave of innovation. As economic tensions continue to rise with China, Chinese-based companies could use their 5G SEPs as international economic weapons to thwart U.S. competitors.

The 5G standard is supposed to be a platform for competition, innovation, and entrepreneurship, but if the Ninth Circuit decision is allowed to stand, it will become a chokepoint for snuffing out competitors and demanding monopoly rents. Open standards and FRAND licensing commitments are fundamental to competition in the modern economy, and the idea that they aren’t a subject for antitrust enforcement is patently absurd.

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

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

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

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

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

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

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

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

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

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

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

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

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

#### Standards leadership allows China to export digital authoritarianism.

Drew et al. 21, \*Dr Alexi Drew, Research Associate, The Policy Institute, King’s College London; (May 7th, 2021, “The Critical Geopolitics of Standards Setting”, https://www.transatlantic-dialogue-on-china.rusi.org/article/the-critical-geopolitics-of-standards-setting)

However, this previously ‘western’ domain is challenged by a Chinese bloc of private industry actors with centrally directed, strategic motivations for their efforts who have managed to leverage the flaws of this system for political and economic advantage.  The market-driven self-regulation model of technical standards has proven itself unsustainable given the geopolitical power achievable through the control of these standards. The marketised approach is easily abusable by a technologically developed nation-state with geopolitical intentions firmly in mind.

Obscurity Through Complexity

Technical standards have the immediate appearance of being both apolitical and ethically neutral. This seems to set them apart from the debate over standards of state behaviour in [cyber space concerning espionage and actions below the threshold of armed conflict](https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what). Yet, technological standards are unequivocally connected to normative practices of international behaviour and ethics. The extremely complex nature of the standards under consideration in bodies such as the International Organization for Standardization, the International Electrotechnical Commission (IEC), the International Telecommunications Union (ITU), and the Third Generation Partnership Project (3GPP) obscures the very tangible real-world impact that the standards they set have. The 3GPP is responsible for standards setting for mobile telecommunications. It covers everything from 5G through to autonomous vehicles and the Internet of Things. These are the bodies defining how the modern world is constructed.

On the one hand they appear quite benign, responsible for such banalities as the use of Universal Serial Bus (USB) connectors versus proprietary standards. This hardly seems a matter of national security importance. But the same process is responsible for what ultimately shape the basic operating parameters of facial recognition technology in closed circuit television systems, the level of centralised state control at the technical foundations of the internet, and the protections of personally identifiable data. These generate profound implications for international policy and ethics.

Internal Competition vs Strategic Direction

Technical standards setting processes have, historically, been dominated by private sector actors who have had both the capacity to develop a particular technology to the point of holding a significant market share, and the ability to use that market share to advocate for the standardisation of the technology in line with their own production. The market led approach has continued to be the prevailing model by which American companies have globalised the technical standards behind US dominated technological innovation. This privatised form of self-regulation for technology companies is only partially influenced by the approach taken within the EU where [some licensing of standards are controlled by state or EU led institutions.](https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2019/ui-brief-no.-2-2019.pdf)

In contrast to this approach the Chinese model has involved a high level of state-oriented direction, oversight, and direct engagement on the creation and signing off technical standards. Efforts to harmonise and centralise technical standards domestically have become increasingly internationalised as the CCP takes this centralised, strategic approach to technical standards setting bodies such as the ITU, 3GPP, and IEC. Technical standards have also become an increasingly central component of the Digital Silk Road with the openly expressed goal of increasing uptake of Chinese technical standards in partner countries.

The implications of this clash between a system of technical standardisation that is driven by the market versus one driven by an authoritarian government subsidised model are a direct challenge to the development of free, open, and ethical technology. Standardisation mechanisms have become political, or rather there has been a gradual realisation of the political power to be gained from the control of technical standards. While the PRC might have come to this awareness first, the US and Europe have since had a rude awakening about the missed opportunity. The privatised model of technical standards setting favoured by European and US markets relies upon the dynamics of financial competition to regulate behaviour. This is in stark contrast to the statist Chinese model.

#### Causes global backsliding.

Kendall-Taylor et. al 20 \*Andrea Kendall-Taylor, senior fellow and director of the Transatlantic Security Program at the Center for a New American Security, co-author of Democracies and Authoritarian Regimes; Erica Frantz is Assistant Professor of Political Science at Michigan State University; Joseph Wright is Professor of Political Science at Pennsylvania State University; (March/April 2020, “The Digital Dictators,” Foreign Affairs, <https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators>)

The risk that technology will usher in a wave of authoritarianism is all the more concerning because our own empirical research has indicated that beyond buttressing autocracies, digital tools are associated with an increased risk of democratic backsliding in fragile democracies. New technologies are particularly dangerous for weak democracies because many of these digital tools are dual use: technology can enhance government efficiency and provide the capacity to address challenges such as crime and terrorism, but no matter the intentions with which governments initially acquire such technology, they can also use these tools to muzzle and restrict the activities of their opponents.

#### Democracy solves a litany of existential threats.

Diamond 19, Professor of Political Science and Sociology at Stanford University, Senior Fellow at the Hoover Institution, Senior Fellow at the Freeman Spogli Institute for International Studies, PhD in Sociology from Stanford University, (Dr. Larry, Ill Winds: Saving Democracy from Russian Rage, Chinese Ambition, and American Complacency, p. 199-202)

The most obvious response to the ill winds blowing from the world’s autocracies is to help the winds of freedom blowing in the other direction. The democracies of the West cannot save themselves if they do not stand with democrats around the world. This is truer now than ever, for several reasons. We live in a globalized world, one in which models, trends, and ideas cascade across borders. Any wind of change may gather quickly and blow with gale force. People everywhere form ideas about how to govern—or simply about which forms of government and sources of power may be irresistible—based on what they see happening elsewhere. We are now immersed in a fierce global contest of ideas, information, and norms. In the digital age, that contest is moving at lightning speed, shaping how people think about their political systems and the way the world runs. As doubts about and threats to democracy are mounting in the West, this is not a contest that the democracies can afford to lose. Globalization, with its flows of trade and information, raises the stakes for us in another way. Authoritarian and badly governed regimes increasingly pose a direct threat to popular sovereignty and the rule of law in our own democracies. Covert flows of money and influence are subverting and corrupting our democratic processes and institutions. They will not stop just because Americans and others pretend that we have no stake in the future of freedom in the world. If we want to defend the core principles of self-government, transparency, and accountability in our own democracies, we have no choice but to promote them globally. It is not enough to say that dictatorship is bad and that democracy, however flawed, is still better. Popular enthusiasm for a lesser evil cannot be sustained indefinitely. People need the inspiration of a positive vision. Democracy must demonstrate that it is a just and fair political system that advances humane values and the common good. To make our republics more perfect, established democracies must not only adopt reforms to more fully include and empower their own citizens. They must also support people, groups, and institutions struggling to achieve democratic values elsewhere. The best way to counter Russian rage and Chinese ambition is to show that Moscow and Beijing are on the wrong side of history; that people everywhere yearn to be free; and that they can make freedom work to achieve a more just, sustainable, and prosperous society. In our networked age, both idealism and the harder imperatives of global power and security argue for more democracy, not less. For one thing, if we do not worry about the quality of governance in lower-income countries, we will face more and more troubled and failing states. Famine and genocide are the curse of authoritarian states, not democratic ones. Outright state collapse is the ultimate, bitter fruit of tyranny. When countries like Syria, Libya, and Afghanistan descend into civil war; when poor states in Africa cannot generate jobs and improve their citizens’ lives due to rule by corrupt and callous strongmen; when Central American societies are held hostage by brutal gangs and kleptocratic rulers, people flee—and wash up on the shores of the democracies. Europe and the United States cannot withstand the rising pressures of immigration unless they work to support better, more stable and accountable government in troubled countries. The world has simply grown too small, too flat, and too fast to wall off rotten states and pretend they are on some other planet. Hard security interests are at stake. As even the Trump administration’s 2017 National Security Strategy makes clear, the main threats to U.S. national security all stem from authoritarianism, whether in the form of tyrannies from Russia and China to Iran and North Korea or in the guise of antidemocratic terrorist movements such as ISIS.1 By supporting the development of democracy around the world, we can deny these authoritarian adversaries the geopolitical running room they seek. Just as Russia, China, and Iran are trying to undermine democracies to bend other countries to their will, so too can we contain these autocrats’ ambitions by helping other countries build effective, resilient democracies that can withstand the dictators’ malevolence. Of course, democratically elected governments with open societies will not support the American line on every issue. But no free society wants to mortgage its future to another country. The American national interest would best be secured by a pluralistic world of free countries—one in which autocrats can no longer use corruption and coercion to gobble up resources, alliances, and territory. If you look back over our history to see who has posed a threat to the United States and our allies, it has always been authoritarian regimes and empires. As political scientists have long noted, no two democracies have ever gone to war with each other—ever. It is not the democracies of the world that are supporting international terrorism, proliferating weapons of mass destruction, or threatening the territory of their neighbors.

#### China 5G leadership compromise US military superiority

Borghard et al. 19, \*Erica D. Borghard is an Assistant Professor at the Army Cyber Institute at West Point. Shawn W. \*Lonergan is a U.S. Army Reserve officer assigned to 75th Innovation Command and a Research Scholar at the Army Cyber Institute. (April 25th, 2019, “The Overlooked Military Implications of the 5G Debate”, https://www.cfr.org/blog/overlooked-military-implications-5g-debate)

There are economic implications for which entities can secure the [greatest global market share](https://www.reuters.com/brandfeatures/venture-capital/article?id=61837) of 5G technology. Technological innovation drives economic growth, job creation, and global economic influence. Huawei may have a long-term market advantage over U.S and Western telecoms because the former has been able to offer 5G products at [far cheaper](https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html) rates than the latter. Furthermore, there are also concerns that Chinese-built 5G technology is likely to [contain backdoors](https://www.wired.com/story/huawei-case-signals-new-us-china-cold-war-tech/) that could be used to enable [Chinese economic or national security espionage](https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html). It is unlikely that Beijing would actively monitor all of the content of the data that comes across Huawei owned or operated infrastructure (although it may collect and analyze metadata). However, it is conceivable that Huawei would get a proverbial “tap on the shoulder” from Beijing to share pertinent information in specific instances. This may include individually targeting senior corporate executives, which is enabled by the millimeter wave frequency that 5G networks employ.

The military applications of 5G technology have vital strategic and battlefield implications for the U.S. Historically, the U.S. military has reaped enormous advantages from employing cutting edge technology on the battlefield. 5G technology holds similar innovative potential. Perhaps most obviously, the next generation of telecommunications infrastructure will have a direct impact on improving military communications. However, it will also produce cascading effects on the development of other kinds of military technologies, such as robotics and artificial intelligence. For instance, artificial intelligence and machine learning capabilities, such as those used in the Department of Defense’s [Project Maven](https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/), could be greatly enhanced when leveraging the data processing speeds made possible through 5G infrastructure. As an [era of great power competition](https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf) emerges between the United States and China, the United States has a compelling strategic interest in being at the forefront of these new technologies.

The United States and its allies must also consider the tactical and operational implications on the battlefield of conducting conventional or counterinsurgency operations in an area with Chinese owned or operated 5G infrastructure. This concern stems from the nature of the relationship between Huawei, an [ostensibly private company](https://www.itnews.com.au/news/analysis-who-really-owns-huawei-175946), and the Chinese Communist Party (CCP). While Huawei’s founder and CEO, Ren Zhengfei proclaimed in a February 2019 interview on [CBS This Morning](https://www.cbsnews.com/news/ren-zhengfei-huawei-ceo-says-we-will-never-provide-chinese-government-with-any-information/)that the company never has and never would provide information to the Chinese government, many experts are [skeptical](https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html). Under China’s [2017 National Intelligence Law](https://www.reuters.com/article/us-china-security-lawmaking-idUSKBN19I1FW), the CCP has the authority to monitor and investigate domestic and international companies as well as direct organizations to assist with government espionage efforts. As such, it is conceivable that Huawei will be required to hand over its data to the Chinese government for collection and analysis.

Due to this reality, the United States must consider and be prepared to conduct overseas contingency or counterterrorism operations in areas where Chinese telecommunications infrastructure is widely proliferated, thus restricting the United States’ ability to rely on indigenous telecoms. As [noted](https://www.africom.mil/media-room/transcript/31604/gen-joseph-votel-gen-thomas-waldhauser-and-acting-asd-for-international-security-affairs-kathryn) by US AFRICOM Commander General Thomas Waldhauser, this has already become an issue in Africa where Chinese telecommunications companies are poised to dominate. The integrity of U.S. military communications systems that rely on 5G networks could be undermined at key phases of an operation. For example, if the United States is conducting a military operation in an area of interest to China, it is plausible that the Chinese government could leverage Huawei to intercept or even deny military communications. Furthermore, Chinese telecom infrastructure dominance in a theater of operations may limit the U.S. military’s ability to conduct precision targeting that leverages signals intelligence collection on 5G telecommunications networks.

The strategic and battlefield implications of who owns and operates 5G infrastructure around the world underscores the national security importance of 5G. The U.S. government and its allies should more systematically assess both the opportunities and risks associated with conducting future military operations in environments that rely on Chinese technology.

To date, the U.S. government has devoted significant energy to persuading its allies and partners to follow the United States in prohibiting Chinese telecoms, particularly Huawei, from building and/or operating 5G infrastructure. However, its diplomatic approach has been met with varying degrees of success. While some countries such as [Australia](https://www.ft.com/content/e90c3800-aad3-11e8-94bd-cba20d67390c) and [Japan](https://www.reuters.com/article/us-usa-china-huawei-japan/japans-top-three-telcos-to-exclude-huawei-zte-network-equipment-kyodo-idUSKBN1O90JW) have fallen in line with the U.S. stance on Huawei, many others have not. The European Commission’s recent 5G [recommendations](https://www.cyberscoop.com/5g-eu-huawei-cybersecurity-recommendations/) for member states dismissed a ban on Chinese telecoms. British intelligence has reportedly maintained that the security risks associated with Huawei can be [sufficiently managed](https://www.ft.com/content/619f9df4-32c2-11e9-bd3a-8b2a211d90d5), and New Zealand, after [initially bandwagoning](https://www.nytimes.com/2018/11/28/business/huawei-new-zealand-papua-new-guinea.html) with the United States in December 2018, abruptly [reversed course](https://www.bloomberg.com/news/articles/2019-02-18/new-zealand-says-china-s-huawei-hasn-t-been-ruled-out-of-5g-role) in February 2019. This is concerning for the United States because New Zealand and the UK are members of the Five Eyes intelligence-sharing alliance. Many allies have refused an outright ban of Huawei because of the company’s ability to offer 5G products at far cheaper rates than Western telecoms.

It is clear that U.S. diplomatic efforts are not working. The reality is that the bottom line is largely driving decision-making. Therefore, rather than take a purely negative approach, the United States should consider using positive inducements to make its 5G products more appealing. While the United States should not strive to mirror China’s top-down approach to innovation, it should work with allies to use market incentives to make U.S.- and Western-developed 5G infrastructure and products more competitive. Furthermore, the U.S. military needs to anticipate that its use of native telecommunications infrastructure in a future operating environment may be compromised, limited, or denied. The U.S. military will inevitably need greater bandwidth on the tactical edge and this should be an imperative that drives investment in research and development to address this challenge.

Technological innovation was at the crux of the United States’ comparative military and economic advantage in the twentieth century. In this contemporary great power competition, U.S. failure to innovate at the scientific and technological frontier will have direct (and deleterious) effects for the United States on the distribution of power in the international system over the long term.

#### Chinese tech superiority upends deterrence and emboldens them to risk conflict over Taiwan---extinction.

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

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

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

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

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

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

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

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

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

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

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

### 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.

#### 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/" \l "_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/" \l "_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/" \l "_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/" \l "_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/" \l "_ftn14)

#### Those attacks cause accidental nuclear escalation.

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

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

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

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

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

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

The Nuclear-Cyber Connection

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

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

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

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

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

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

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

Pathways to Escalation

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

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

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

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

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

### 1AC---Solvency

#### 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.

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

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

3. Application of the Basic Legal Principles

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# 2ac

## Solvency

**Biden’s XO solves---he’s devoting all resources on deck to prosecuting antitrust.**

**Posner 21**, professor at the University of Chicago Law School (Eric, 7-21-2021, "The Antitrust War’s Opening Salvo", Project Syndicate, <https://www.project-syndicate.org/commentary/biden-antitrust-executive-order-what-it-does-by-eric-posner-2021-07>. Accessed 7-22-21)

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

The order also establishes a **new bureaucratic organization** in the White House to lead the anti-monopoly effort. Demanding a **“whole-of-government”** approach, it calls on the **vast resources** of **numerous agencies**, and not just the two that traditionally oversee antitrust (the **D**epartment **o**f **J**ustice and the **F**ederal **T**rade **C**ommission).

## 2ac –DOJ

**2AC---AT: DOJ Enforcement DA---TL**

**Turn---the DOJ is already prepared to engage in more antitrust litigation over SEP’s---tradeoffs inevitable.**

**Love 21**, \*Bruce Love, writer at the National Law Journal; (June 15th, 2021, “As DOJ Confirms a Change in Antitrust Patent   
Policy, Lawyers Prepare for Shifting Demand”, https://www.mckoolsmith.com/assets/htmldocuments/2021%2006%2016%20As%20DOJ%20Confirms%20a%20Change%20in%20Anittrust%20Patent%20Policyk%20Lawyers%20Prepare%20for%20Shifting%20Demand%20-%20The%20National%20Law%20Journal.pdf)

The Justice Department has confirmed it is looking to develop **new policies** surrounding how **standard-essential patents** might be used as tools for **anticompetitive practices**. The change in policy will mean big business for law firms that can combine highly technical IP advice with their antitrust and litigation practices, with one lawyer likening the demanding skill set to “three-dimensional chess.” Standard-essential patents, or SEPs, are a fundamental piece of intellectual property for business and innovation because they are used under license so frequently by manufacturing companies other than the patent owners. The policy change was hinted at during an online event in late May, when Richard Powers, the acting attorney general of DOJ’s antitrust division, gave an indication that the government might be **walking back** the **relaxed approach** implemented by the DOJ under the **Trump administration**. A DOJ spokesperson confirmed in an email Tuesday to Law.com that it will **change its policy** on **SEPs** and **antitrust behavior**, with the agency still working out the details. The new administration, said the DOJ spokesperson, is rethinking what policies at the intersection of IP and anti- trust will best serve competition and consumers. “New Department leadership is working with career staff on developing a more balanced approach,” said the DOJ spokesperson. “The department wants to develop neutral and balanced policies in this area that recognize the importance of both antitrust enforcement and JUNE 15, 2021 As DOJ Confirms a Change in Antitrust Patent Policy, Lawyers Prepare for Shifting Demand BY BRUCE LOVE U.S. law has often **shied away** from enforcing essential patent obligations. **That’s set to change**. The result could be “a significant change in the volume and nature of business for IP trial lawyers and their clients,” one lawyer said. Office of the Attorney General at the U.S. Department of Justice in Washington, D.C. June 6, 2020. THE NATIONAL LAW JOURNAL JUNE 15, 2021 intellectual property protection to our economy and that do not favor one set of interests over others.” Such policy changes could result in a swell of business for law firms with deep, technical IP benches and strong experience representing the industry in enforcement actions, lawyers said. Trump’s DOJ had “**taken its foot off the gas**” when it came to SEPs as the focus of anti-competitive behavior, said one Washington-based lawyer, speaking on the condition of anonym- ity because he currently has active cases that involve both SEP enforcement and defense. “It didn’t mean we weren’t busy as litigators. There was a lot of work enforcing SEPs against infringers and defending against infringement allegations,” he said. “But we **weren’t busy** in the **antitrust** arena. A **greater focus** on SEPs—not just by the DOJ but also other agencies—might mean **more litigation**, but it will also mean a more transparent field of play. It doesn’t do companies any good for there to be unfettered SEP enforcement.”

**The prospect of antitrust intervention deters violations---that’s Melamed and Shapiro---no enforcement necessary.**

**Cheng 13**, \*Thomas Cheng, B.A. (Yale), J.D. (Harvard), B.C.L. (Oxon); Attorney & Counsellor, New York State; Associate Professor, Faculty of Law, The University of Hong Kong; (2013, “Putting Innovation Incentives Back in the Patent-Antitrust Interface”, <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1195&context=njtip>), ability edited

Imposing a duty to license on opportunistic patentees may solve this problem. If these patentees know that the **courts may step in** and **mandate licensing** at a **reasonable royalty rate**,214 they will be **induced** to enter into **negotiations** with **follow-on innovators** in **good faith**.215 The threat of compulsory licensing may become a default background legal rule against which negotiations between initial and follow-on innovators take place. The **instances** in which the **courts need to intervene** could be **few**.

**(READ EARLIER) Biden’s XO solves---he’s devoting all resources on deck to prosecuting antitrust.**

**Posner 21**, professor at the University of Chicago Law School (Eric, 7-21-2021, "The Antitrust War’s Opening Salvo", Project Syndicate, <https://www.project-syndicate.org/commentary/biden-antitrust-executive-order-what-it-does-by-eric-posner-2021-07>. Accessed 7-22-21)

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

The order also establishes a **new bureaucratic organization** in the White House to lead the anti-monopoly effort. Demanding a **“whole-of-government”** approach, it calls on the **vast resources** of **numerous agencies**, and not just the two that traditionally oversee antitrust (the **D**epartment **o**f **J**ustice and the **F**ederal **T**rade **C**ommission).

## States CP---2AC

#### 1---Permutation do both---solves politics, concurrent action lets the fed deflect blame on the states.

#### 2---Fifty-state fiat destroys equity and fairness---it’s a stacked deck that allows multi-actor fiat in unrealistic ways and makes generating solvency deficits impossible absent a stable lit base.

#### 3---Perm do the CP---uniform fiat changes antitrust law in the entire US

#### 4---Pre-emption deficit---

#### A---The Ninth Circuit imposed court-order limitations on antitrust law to preserve its balance with patent law.

Martino et al. 20, \*[Matthew M. Martino](https://www.skadden.com/professionals/m/martino-matthew-m) [Tara L. Reinhart](https://www.skadden.com/professionals/r/reinhart-tara-l) [Steven C. Sunshine](https://www.skadden.com/professionals/s/sunshine-steven-c) [Julia K. York](https://www.skadden.com/professionals/y/york-julia-k), works with clients at Skadden, Arps, Slate, Meagher & Flom LLP; (August 14th, 2020, “Ninth Circuit Strikes Down Sweeping Injunction Against Qualcomm and Reins In Expansive Interpretation of Sherman Act”, https://www.skadden.com/insights/publications/2020/08/ninth-circuit-strikes-down-sweeping-injunction)

In its highly anticipated decision, the Ninth Circuit panel unanimously rejected the lower court’s reasoning, vacating the judgment and reversing the worldwide injunction against Qualcomm. The panel concluded that the district court had erroneously imposed the antitrust duty to deal on Qualcomm, had impermissibly looked outside the relevant antitrust market in order to infer an anticompetitive act and had relied on outdated evidence of agreements that were terminated before the suit was filed to justify a broad, forward-looking global injunction. The Ninth Circuit further rejected the argument that a SEP holder’s violation of FRAND commitments could independently create antitrust liability, instead pointing to patent and contract law as sources for potential remedies. The decision reflects a considered effort to rei

n in the district court’s expansive interpretation of general antitrust principles and their specific application to SEP holders, as well as recognition that the antitrust laws aim to preserve companies’ incentives to innovate and compete. Recognizing that while “[a]nticompetitive behavior is illegal under federal antitrust law[,]” the panel was adamant that “[h]ypercompetitive behavior is not.”[7](https://www.skadden.com/insights/publications/2020/08/ninth-circuit-strikes-down-sweeping-injunction" \l "ftn7)

Rejection of District Court’s Expansive Interpretation of Antitrust Laws

The Ninth Circuit decision contains several notable conclusions regarding the scope of Section 2 of the Sherman Act and what constitutes cognizable antitrust harm.

#### B---Any confliction with patent law will be preempted.

Richard A. Samp 14, Chief Counsel of the Washington Legal Foundation, a nonprofit public interest law firm located in Washington, D.C., graduate of Harvard College and the University of Michigan Law School, 2014, “The Role of State Antitrust Law in the Aftermath of Actavis,” https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1062&context=mjlst

On the other hand, state antitrust laws—like all state laws—are subject to the restrictions imposed by the Supremacy Clause of the U.S. Constitution,15 and are impliedly preempted to the extent that they conflict with federal law.16 Such a conflict arises when “compliance with both federal and state regulations is a physical impossibility,”17 or when a state law “stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.”18 On a number of occasions, the Supreme Court has concluded that state antitrust law is preempted because it conflicts with a federal statute other than federal antitrust law.19 The Court has been particularly quick to find preemption when state antitrust law has an impact on labor law, an area in which federal law is pervasive.20 Indeed, on at least one occasion, the Court found that a claim arising under state antitrust law was preempted by federal labor law even though the Court concluded that the conduct that gave rise to the state claim could proceed as a claim under federal antitrust law.21 The Court explained that “Congress and this Court have carefully tailored the antitrust statutes to avoid conflict with the labor policy favoring lawful employee organization, not only by delineating exemptions from antitrust coverage but also by adjusting the scope of the antitrust remedies themselves.”22 The Court said that state antitrust laws “generally have not been subjected to this process of accommodation” and thus that “[t]he use of state antitrust law . . . [must] be pre-empted because it creates a substantial risk of conflict with policies central to federal labor law.”23 Accordingly, in any challenge to a “reverse payment” patent settlement arising under state antitrust law, a court will likely be required to address whether the claim conflicts with the “balance” between federal antitrust law and federal patent law established by the Supreme Court’s Actavis decision. If such state-law antitrust claims stand as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress in adopting the patent laws, it will be preempted by federal law.

## Reg Cp

### 2AC---AT: Regulation CP---TL

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

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

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

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

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

I. The Relative Efficiency of Antitrust and Regulation

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

Relative expertise.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Evading regulatory limits as antitrust harm

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

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

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

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

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

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

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

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

#### \*Deterrence matters---SEP holders will remain opportunistic absent the threat of antitrust.

Tsilikas 17, \*Haris Tsilikas is an IP and Antitrust Consultant, a Doctoral Candidate and Visiting Research Fellow at the Max Planck Institute for Innovation and Competition, Munich; (2017, Antitrust Enforcement and Standard Essential Patents: Moving beyond the FRAND Commitment”, https://www.jstor.org/stable/pdf/j.ctv941t01.9.pdf?refreqid=excelsior%3A92dc720d1ebc7088811b40032a60f575)

Antitrust could play a meaningful role.165 The most important contribution of antitrust enforcement against abuses of SEPs is its deterrent effect.166 Although patent law reforms or contractual binding of subsequent SEPs-holders to FRAND licensing would provide to victims of hold-up useful defences in court, they do not sufficiently deter abusive assertion of SEPs in the first place. For instance, the contractual binding to FRAND could raise counterclaims of breach of contract or/and contractual performance; however, the opportunistic SEP-holder will, in case it loses on such grounds, be left no worse than with a licence on FRAND terms. In the end, a patent hold-up is indeed precluded, but contractual constraints can do little to prevent opportunistic assertion of SEPs in the first place. The victims still suffer the costs of uncertain and resource-draining litigation; most importantly, the reliability of the standards-setting process might still be at risk.

Antitrust enforcement on the other hand, in imposing tortfeasors positive monetary losses in the form of fines, alters the profit-cost calculus of opportunistic behaviour in the first place; opportunistic assertion of SEPs will come at a cost. Of course, a too-heavy-handed approach could have a chilling effect on legitimate patent assertions against implementers that are reluctant to pay FRAND royalties, thus leading to false positives. Antitrust enforcement should carefully examine the specificities of each case, such as the particular PAE conduct, the relationship between PAEs and practicing entities, the structure of downstream markets.167 More importantly, an economically informed antitrust analysis focusing on the actual and potential anticompetitive effects of opportunistic SEPs assertion should prohibit behaviour that is truly harmful to consumers. Safeguarding the inclusive and efficient character of the standards-setting process is a competition law problem. Informed antitrust analysis could provide adequate responses to opportunistic PAE behaviour and privateering.

### 2AC---No Regulation---Patent Holdup

#### No regulatory regime exists for SSO patent holdup---the counterplan doesn’t exist!

Cary et al. 11, \*Messrs. George Cary and Alex Sistla are members of the California and District of Columbia Bars. Mr. Mark Nelson is a member of the New York and District of Columbia Bars. Mr. Steven Kaiser is a member of the New Jersey and District of Columbia Bars; (2011, “THE CASE FOR ANTITRUST LAW TO POLICE THE PATENT HOLDUP PROBLEM INSTANDARD SETTING”, <https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/publication-pdfs/the-case-for-antitrust-law-to-police-the-patent-holdup-problem-in-the-standard-setting.pdf>)

B. IMPLIED PREEMPTION DOCTRINE DOES NOT APPLY TO PATENT HOLDUP

Even accepting the idea of implied preemption in the face of substantial regulatory regimes, the case for preempting the antitrust laws in the SSO-patent holdup context has not been made. Put simply, there is no regulatory oversight in the case of SSO-patent holdup. Although the Patent and Trade-mark Office (PTO) regulates patents in the sense of deciding what patents to issue, there is no connection between that role and the patent holdup issue. Indeed, almost every dispute involving a patent—whether patent abuse, infringement, or licensing quarrels—is ordinarily resolved through some form of private litigation or dispute resolution.79

It is of course true that there is a specialized patent court (the Federal Circuit), and that certain doctrines (laches, equitable estoppel, and misuse) have been developed to address “opportunistic behavior” by patentees. But this simply means that there is an independent body of patent law that certain private parties may enforce. The government does not actively police the behavior of patent holders in the way the SEC enforces the securities laws or the states enforce their laws in the state-action context.80 Although the PTO imposes certain duties upon patent applicants,81 it lacks the authority to impose any such similar duties upon patentees participating in a standard-setting process. SSOs impose their own disclosure obligations without any interference or oversight by the PTO. In sum, we think it is a stretch to argue that a competing regulatory scheme governs all of patent law. Many patent law defenses, such as those recognized under 35 U.S.C. § 282, are borrowed from the common law.

## BizCon Da

#### Business confidence low.

Goll 8/24/21, \*Vince Goll; (August 24th, 2021, “US business confidence slows to an eight month low on supply woes”, https://www.independent.ie/business/world/us-business-confidence-slows-to-an-eight-month-low-on-supply-woes-40780967.html)

US business activity continues to downshift, with growth slowing to an eight-month low in August against a backdrop of materials shortages, a lack of labor and an upswing in coronavirus infections.

The IHS Markit flash August composite index of purchasing managers at services and manufacturers dropped to 55.4 from 59.9 a month earlier, the group reported yesterday. Readings above 50 indicate growth and the gauge has decreased each month since hitting a record 68.7 in May.

The pullback this month underscores the extent to which supply chain disruptions are hammering firms already struggling to meet demand. Service providers and manufacturers continue to face challenges attracting workers and obtaining the supplies they need.

At factories, for instance, an IHS gauge of supplier deliveries showed the longest lead times in records back to 2007.

"Not only have supply chain delays hit a new survey record high, but the August survey saw increasing frustrations in relation to hiring," Chris Williamson, chief business economist at IHS Markit, said.

"Jobs growth waned to the lowest since July of last year as companies either failed to find suitable staff or existing workers switched jobs."

Limited capacity is translating into sustained inflationary pressures as well. The group's composite index of input prices increased in August to the second-highest reading in data back to 2009. A measure of prices received also advanced, indicating companies are having some success passing along higher costs.

The IHS Markit index of services activity declined to show the slowest pace of growth since December, while a measure of new business dropped to a one-year low.

#### COVID-19, worker shortages, and supply chain disruptions hurt business confidence.

Geehern 9/6/21, \*Chris Geehern; COVID, (September 6th, 2021, “Worker Shortages Dampen Business Confidence”, https://aimnet.org/blog/covid-worker-shortages-dampen-business-confidence/)

Resurgent COVID-19 cases, persistent worker shortages and supply chain disruptions combined to dampen business confidence in Massachusetts during August.

The Associated Industries of Massachusetts Business Confidence Index (BCI) declined 3.6 points to 62.0 after hitting a three-year high during July. The BCI remains 16 points higher than a year ago.

Employers grew less optimistic last month about everything from their own companies to the state and national economies. Confidence among manufacturing companies declined for the first time this year as companies faced the twin challenges of surging prices and shortages of key raw materials.

The report came as hiring nationally slowed sharply during August to 235,000 jobs.

“Business owners and managers remain solidly optimistic overall, but express growing concern as COVID-19 cases increase both in Massachusetts and globally,” said Sara L. Johnson, Chair of the AIM Board of Economic Advisors and Executive Director of Global Economics at IHS Markit.

“Everyone from manufacturers to retailers is struggling to provide product amid renewed pandemic-containment measures and critical shortages of labor and materials.”

Employers say supply chain issues have become a drag on an otherwise solid economy.

“The supply chain lead-times are killing our ability to drive business in the short-term.  Trying to get key supplies on a container is impossible so our costs keep going up due to having to airfreight parts in,” wrote one employer.

The AIM Index, based on a survey of more than 140 Massachusetts employers, has appeared monthly since July 1991. It is calculated on a 100-point scale, with 50 as neutral; a reading above 50 is positive, while below 50 is negative. The Index reached its historic high of 68.5 on two occasions in 1997-98, and its all-time low of 33.3 in February 2009.

Constituent Indicators

The constituent indicators that make up the Business Confidence Index all moved lower during August.

The confidence employers have in their own companies fell 5.0 points to 62.7, leaving it 13.7 points better than it was during the pandemic a year ago.

#### Low confidence now hurts investment prospects.

Zandi 8/18/21, \*Mark Zandi, CNN Business Perspectives; (August 18th, 2021, “Here's what the Delta variant means for the economic recovery”, https://www.actionnewsnow.com/content/national/575121712.html)

Businesses have also suddenly become more nervous. According to Moody's Analytics weekly [business confidence index](https://www.economy.com/economicview/indicator/usa_dsbc/DFBA2A45-8167-4D14-8763-EE4F343ACD15/World-Moodys-Analytics-Survey-of-Business-Confidence), sentiment had significantly improved this spring when vaccinations ramped up and the pandemic was steadily winding down. But it has gone sideways since mid-June. Businesses' assessment of current conditions has turned particularly soft in the past few weeks, with more survey respondents saying conditions are weakening than those that say they are improving. This is the first time this has happened since the vaccines became widely available.

Businesses' expectations regarding the economy's prospects for the remainder of this year have also diminished significantly. The number of respondents that say the economy will continue to improve has declined from more than 60% to less than half, and those that say the economy will weaken has increased from near 30% to more than 40%. This hasn't impacted businesses' hiring and investment decisions yet, according to our survey, but it bears close watching, as the job market and broader economic recovery would be in jeopardy if businesses pull back on hiring and investments.

#### No correlation between economic decline and war.

Walt 20, Robert and Renée Belfer professor of international relations at Harvard University. (Stephen M., 5/13/20, “Will a Global Depression Trigger Another World War?”, *Foreign Policy*, https://foreignpolicy.com/2020/05/13/coronavirus-pandemic-depression-economy-world-war/)

On balance, however, I do not think that even the extraordinary economic conditions we are witnessing today are going to have much impact on the likelihood of war. Why? First of all, if depressions were a powerful cause of war, there would be a lot more of the latter. To take one example, the United States has suffered 40 or more recessions since the country was founded, yet it has fought perhaps 20 interstate wars, most of them unrelated to the state of the economy. To paraphrase the economist Paul Samuelson’s famous quip about the stock market, if recessions were a powerful cause of war, they would have predicted “nine out of the last five (or fewer).”   
Second, states do not start wars unless they believe they will win a quick and relatively cheap victory. As John Mearsheimer showed in his classic book Conventional Deterrence, national leaders avoid war when they are convinced it will be long, bloody, costly, and uncertain. To choose war, political leaders have to convince themselves they can either win a quick, cheap, and decisive victory or achieve some limited objective at low cost. Europe went to war in 1914 with each side believing it would win a rapid and easy victory, and Nazi Germany developed the strategy of blitzkrieg in order to subdue its foes as quickly and cheaply as possible. Iraq attacked Iran in 1980 because Saddam believed the Islamic Republic was in disarray and would be easy to defeat, and George W. Bush invaded Iraq in 2003 convinced the war would be short, successful, and pay for itself.

The fact that each of these leaders miscalculated badly does not alter the main point: No matter what a country’s economic condition might be, its leaders will not go to war unless they think they can do so quickly, cheaply, and with a reasonable probability of success.

Third, and most important, the primary motivation for most wars is the desire for security, not economic gain. For this reason, the odds of war increase when states believe the long-term balance of power may be shifting against them, when they are convinced that adversaries are unalterably hostile and cannot be accommodated, and when they are confident they can reverse the unfavorable trends and establish a secure position if they act now. The historian A.J.P. Taylor once observed that “every war between Great Powers [between 1848 and 1918] … started as a preventive war, not as a war of conquest,” and that remains true of most wars fought since then.

The bottom line: Economic conditions (i.e., a depression) may affect the broader political environment in which decisions for war or peace are made, but they are only one factor among many and rarely the most significant. Even if the COVID-19 pandemic has large, lasting, and negative effects on the world economy—as seems quite likely—it is not likely to affect the probability of war very much, especially in the short term.

# 1ar

## adv – 2

### 1AR---UQ---Solarwinds

#### SolarWinds serves as a beachhead for future attacks---it’s scale was unprecedented.

Muggah 21, \*Robert Muggah is a political scientist, urbanist and security expert. He is the co-founder of the Igarapé Institute and The SecDev Group, where he is known for his work on urbanization, crime prevention, arms control, migration, cyber-security, the digital economy, conflict and development studies; (January 11th, 2021, “Why The Latest Cyberattack Was Different”, https://foreignpolicy.com/2021/01/11/cyberattack-hackers-russia-svr-gru-solarwinds-virus-internet/)

What sets the SolarWinds attack apart from previous incidents is its sheer scale. The company has over 300,000 customers worldwide, [according to filings](https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm) made to the U.S. Securities and Exchange Commission. Throughout 2020, SolarWinds sent out software updates to roughly [18,000 of them](https://www.computing.co.uk/news/4024968/solarwinds-fewer-customers-installed-malware-laced-orion-software-update-led-us-treasury-hack). To date, [at least 250](https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html) networks have reportedly been affected by the booby-trapped file. Shortly after being downloaded, the virus executes commands that create a backdoor in the network to transfer files, disable services, and reboot machines. Targeted institutions [include](http://r/) the U.S. departments of Defense, Homeland Security, State, Energy, and the Treasury; all five branches of the U.S. military; the National Nuclear Security Administration, and 425 of the Fortune 500 companies, including [Cisco](https://www.itproportal.com/news/it-giants-vmware-cisco-confirmed-as-victims-of-solarwinds-hack/), Equifax, [MasterCard](https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12), and [Microsoft](https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/). There have been other major cyberattacks in the past, but none has achieved this kind of penetration. By compromising powerful governments and businesses, including some of the [most successful technology companies](https://www.forbes.com/sites/antoinegara/2020/12/18/solarwinds-hack-throws-wrench-in-private-equitys-most-profitable-market/?sh=5dea5fc6ef73), the SolarWinds exploit shatters the illusion of information security. The hack has also [spooked](https://www.bloomberg.com/news/articles/2020-12-18/banks-on-alert-after-first-sweep-finds-no-evidence-of-major-hack) the financial services sector.

Within hours of the attack’s discovery, U.S. government officials and cybersecurity experts singled out [Russia’s Foreign Intelligence Service](https://www.businessinsider.com/krebs-solarwinds-cybersecurity-hack-more-broad-2020-12) (known as the SVR) as the likely culprit. Its elite hacking unit, known in cybersecurity circles as [APT29 or “Cozy Bear](https://www.cyberscoop.com/cozy-bear-apt29-solarwinds-russia-persistent/),” is a familiar adversary. It was reportedly behind digital breaches of the White House, State Department, and Joint Chiefs of Staff in 2014 and 2015, as well as the infamous hack of the Democratic National Committee during the 2016 election campaign. The SVR hacked the party’s servers alongside another Russian team, APT28 or “Fancy Bear,” which is overseen by Russia’s military intelligence agency, commonly known as the GRU. It was the GRU that reportedly stole Democratic campaign emails and dumped them online; in 2018, the U.S. Department of Justice [indicted 12 Russians](https://abcnews.go.com/Politics/12-russian-intel-officers-indicted-dnc-hacking-mueller/story?id=56564708) suspected of involvement. A few days after the SolarWinds compromise became public, the U.S. Cybersecurity and Infrastructure Security Agency [warned](https://us-cert.cisa.gov/ncas/alerts/aa20-352a) that the hack “poses a grave risk” to federal, state, and local governments, as well as to private companies.

This is not an open-and-shut case, however. One of the most frustrating challenges for victims of cyberespionage and cyberwarfare is the difficulty of attributing an attack. While the SolarWinds exploit was linked to the SVR in a [joint statement](https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure) by U.S. intelligence agencies, it is by the attack’s very nature impossible to be certain. Complicating matters, another piece of malware that targeted SolarWinds at around the same time—dubbed Supernova by [Palo Alto Networks’ Unit 42](https://unit42.paloaltonetworks.com/solarstorm-supernova/)—appears to have been planted by [another actor](https://www.zdnet.com/article/a-second-hacking-group-has-targeted-solarwinds-systems/). Meanwhile, US investigators are exploring the [possible involvement of JetBrain](https://www.zdnet.com/article/jetbrains-denies-being-involved-in-solarwinds-hack/), a Czech firm founded in Russia that counts SolarWinds among its clients, in spreading infected code via its [TeamCity product](https://blog.jetbrains.com/teamcity/2021/01/statement-on-the-story-from-the-new-york-times-regarding-jetbrains-and-solarwinds/). For its part, the Russian Embassy in Washington [posted](https://www.facebook.com/RusEmbUSA/posts/1488755328001519) a statement on Facebook denying responsibility and claiming that the attacks were opposed to Russia’s foreign-policy interests. It also added that “Russia does not conduct offensive operations in the cyber domain.” Contradicting his own secretary of state and intelligence services, U.S. President Donald Trump [agreed](https://www.businessinsider.com/solarwinds-software-cybersecurity-breach-trump-russia-china-pompeo-technology-2020-12) with the Russians, hinting that China might be to blame.

What also makes the SolarWinds breach different from past attacks was how it was delivered, and the way it could serve as a beachhead for future attacks. Unlike in the case of high-profile phishing and hacking exploits against companies such as [Equifax](https://www.cnet.com/news/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/) and [Sony](https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea), it is exceedingly difficult to trace how the SolarWinds compromise occurred and determine which data was accessed and pilfered. That’s because the victims of the SolarWinds attack were not confined to a single organization or department, and it is not possible to simply eliminate the malware by wiping the system clean. To the contrary: Hackers ensured that they would have long-term access by adding new credentials and using administrative privileges to grant themselves permissions to access various parts of their victims’ IT infrastructure. What this means is that this hyper-sophisticated campaign—including the theft of information from protected networks—could go on for years.

Even more ominously, the SolarWinds attack is what’s known in security circles as a cascading supply chain compromise—which means that it stretches [far beyond](https://www.wired.com/story/russia-solarwinds-supply-chain-hack-commerce-treasury/) the company’s own direct clients. While no one yet knows just how many governments and businesses are affected, tens of thousands of other entities are at risk, many of which have little to do with SolarWinds. And because the company’s products are designed to monitor digital networks and are therefore at the very heart of IT infrastructure, they have extensive access and few constraints on their reach. Making matters worse, SolarWinds reportedly encouraged customers to relax existing antivirus and security restrictions, which means that even more of the network was accessible than usual. Attackers made use of this unrestricted access to steal permissions and source code from companies such as [Microsoft](https://www.cnbc.com/2021/01/01/solarwinds-hackers-accessed-microsoft-source-code-the-company-says.html) and compromise even more targets.

The exploit is a reminder of the blurred lines between espionage and warfare, and the difficulty of formulating a proportional response. As diplomats know well, there is no established international norm against espionage—clandestine information collection is a tolerated feature of international relations. When spying is publicly exposed, what typically follows are some form of condemnation, sanctions, and a focus on shoring up defenses to keep it from happening again. However, the vast scale of the SolarWinds exploit—and the strong probability of others like it that have yet to be detected—should force a rethink. The potential for weaponizing compromised systems, including by sabotaging public utilities (as was the case in a recent [cyberattack tit-for-tat between Israel and Iran](https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/)), poses an existential threat.

### 1AR---!---Rational Escalation

#### Irrespective of the “fog of war”, NC3 penetration creates rational incentives to escalate.

Gartzke et al. 17, \*Erik Gartzke is Professor of Political Science and Director of the Center for Peace and Security Studies (cPASS) at the University of California, San Diego, where he has been a member of the research faculty since 2007; \*Jon R. Lindsay is Assistant Professor of Digital Media and Global Affairs at the Munk School of Global Affairs and Public Policy and the Department of Political Science at the University of Toronto. He is the co-editor of Cross-Domain Deterrence and China and Cybersecurity; (March 2017, “Thermonuclear cyberwar”, <https://academic.oup.com/cybersecurity/article/3/1/37/2996537#64534849>)

The outcome of fog of decision scenarios such as these depend on how humans react to risk and uncertainty, which in turn depends on bounded rationality and organizational frameworks that might confuse rational decision making [[89](javascript:;), [90](javascript:;)]. These factors exacerbate a hard problem. Yet within a rationalist framework, cyber attacks that have already created their effects need not trigger an escalatory spiral. While being handed a fait accompli may trigger an aggressive reaction, it is also plausible that the target’s awareness that its NC3 has been compromised in some way would help to convey new information that the balance of power is not as favorable as previously thought. This in turn could encourage the target to accommodate, rather than escalate. While defects in rational decision making are a serious concern in any cyber–nuclear scenario, the situation becomes even more hazardous when there are rational incentives to escalate. Although “known unknowns” can create confusion, to paraphrase Donald Rumsfeld, the “unknown unknowns” are perhaps more dangerous.

A successful clandestine penetration of NC3 can defeat the informational symmetry that stabilizes nuclear relationships. Nuclear weapons are useful for deterrence because they impose a degree of consensus about the distribution of power; each side knows the other can inflict prohibitive levels of damage, even if they may disagree about the precise extent of this damage. Cyber operations are attractive precisely because they can secretly revise the distribution of power. NC3 neutralization may be an expensive and rarified capability in the reach of only a few states with mature signals intelligence agencies, but it is much cheaper than nuclear attack. Yet the very usefulness of cyber operations for nuclear warfighting ensure that deterrence failure during brinksmanship crises is more likely.

Nuclear states may initiate crises of risk and resolve to see who will back down first, which is not always clear in advance. Chicken appears viable, ironically, because each player understands that a nuclear war would be a disaster for all, and thus all can agree that someone can be expected swerve. Nuclear deterrence should ultimately make dealing with an adversary diplomatically more attractive than fighting, provided that fighting is costly—as would seem evident for the prospect of nuclear war—and assuming that bargains are available to states willing to accept compromise rather than annihilation. If, however, one side knows, but the other does not, that the attacker has disabled the target’s ability to perceive an impending military attack, or to react to one when it is underway, then they will not have a shared understanding of the probable outcome of war, even in broad terms.

Consider a brinksmanship crisis between two nuclear states where only one has realized a successful penetration of the rival’s NC3. The cyber attacker knows that it has a military advantage, but it cannot reveal the advantage to the target, lest the advantage be lost. The target does not know that it is at a disadvantage, and it cannot be told by the attacker for the same reason. The attacker perceives an imbalance of power while the target perceives a balance. A dangerous competition in risk taking ensues. The first side knows that it does not need to back down. The second side feels confident that it can stand fast and raise the stakes far beyond what it would be willing to if it understood the true balance of power. Each side is willing to escalate to create more risk for the other side, making it more likely that one or the other will conclude that deterrence has failed and move into warfighting mode to attempt to limit the damage the other can inflict.

### 1AR---!---Positive Feedback

#### Positive feedback loops causes cyber-competition to spiral out of control.

Jervis et al. 20, \*Robert Jervis (Ph.D., California at Berkeley, 1968) is the Adlai E. Stevenson Professor of International Politics and has been a member of the Columbia political science department since 1980; \*Jason Healey is a senior research scholar and adjunct professor at the School of International and Public Affairs, Columbia University. He is also a senior fellow with the Cyber Statecraft Initiative at the Atlantic Council, where he was the program's founding director; (Fall 2020, “The Escalation Inversion and Other Oddities of Situational Cyber Stability”, https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/)

Next Steps for Situational Cyber Stability

In the film comedy Zoolander, a group of not-too-bright male models have a gasoline fight at a filling station. Everyone watching is in on the joke: It is only a matter of time before one of these imbeciles, oblivious to the danger, lights a match. The punchline, a massive fireball, is a surprise to no one.

We hope this analogy to cyber conflict remains a silly one — there is no comparison to states playing a dangerous game, soaked in vulnerabilities and being complacent that no one will light up. But the dynamics of cyber conflict drive nearly all states to be greedy, expansionist powers. Every adversary is deeply vulnerable and obeying broadly the same imperatives — to collect intelligence, lay the groundwork for future attacks, and seize terrain in cyberspace to contest an adversary’s operations — and assuming all others are maximally doing the same.[132](https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/" \l "_ftn132) This competition is not carried out over physical territory, but over network infrastructure and information, owned by the private sector and the lifeblood of modern economy and society.  This drives positive feedback, possibly spiraling out of the willful control of the participants.[133](https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/" \l "_ftn133)

If states are frustrated in the competition to achieve meaningful strategic gains through cyberspace, this may just fuel additional escalation. Each side will go back to their legislatures or paymasters, asking for a larger budget and looser rules and pointing to the other side’s newly aggressive forward defense as proof of their intransigence. Since each side views the other as aggressive, there is “no reason to examine one’s own policies,” nor is there a “need to make special efforts to demonstrate willingness to reach reasonable settlements.”[134](https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/" \l "_ftn134) If concessions will not alter the other’s actions, then restraint can seem a fool’s choice — unless everyone is soaking in gasoline.

Stability and restraint may not be likely unless adversaries seek stability and act with restraint. This will be particularly hard now that the participants are engaged in relentless, persistent engagements. Conflict (especially conflict that can never really end, like that in cyberspace) can lead to heightened emotions, unwillingness to compromise, and self-righteousness.[135](https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/" \l "_ftn135) The United States believes, probably rightly, that it has showed restraint by eschewing large-scale disruptive operations or espionage for commercial gain, and sets great store in how this restraint highlights U.S. interests for a peaceful cyberspace. But these self-imposed limits have been overshadowed by near-limitless political-military espionage. American claims that its “pervasive, persistent access on the global network” is “just espionage” fall flat.[136](https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/" \l "_ftn136) Adversaries (and allies) could be forgiven for doubting U.S. restraint, given their existential dependence on technology largely invented and created in a country seeking to bask in lasting cyberspace pre-eminence.

## cp – reg neg

## da – bizcon

### 1AR---UQ---BizCon

#### 3 --- Delta variant has tanked confidence

**Simon 8-13** (Ruth Simon, 8-13-2021, WSJ, "WSJ News Exclusive | Delta Variant Drops Small-Business Confidence to Lowest Level Since March ", https://www.wsj.com/articles/delta-variant-drops-small-business-confidence-to-lowest-level-since-march-11628868656)

Small-business confidence dropped in August to its lowest level since early spring, as the rise in Covid-19 cases due to the highly transmissible Delta variant put a damper on expectations and turned entrepreneurs more cautious.

Thirty-nine percent of small-business owners expect economic conditions in the U.S. to improve in the next 12 months, down from 50% in July and 67% in March, according to a survey of more than 560 small businesses for The Wall Street Journal by Vistage Worldwide Inc., a business coaching and peer advisory firm.

The measure is one part of a broader confidence index that also tracks metrics such as small-business owners’ outlook for their companies and their investment and hiring plans. That overall figure remains positive, but fell to its lowest level since March.

#### 4 --- Business confidence declining---delta variant.

Tappe 7-28-21, senior writer at CNN Business, covering financial markets and the U.S. economy; (Anneken, “The economy is still not back to normal. The Delta variant won't make it easier”, https://www.cnn.com/2021/07/28/economy/economy-delta-variant-gdp-forecast/index.html)

New York (CNN Business) America's economy isn't [back to normal](https://www.cnn.com/business/us-economic-recovery-coronavirus) yet, and much of the recovery depends on consumers: how much [they're spending](http://www.cnn.com/2021/07/26/economy/goldman-sachs-services-economy-delta/index.html), how much they decide to participate in public life and even whether they work remotely. And while economists don't believe a full shutdown is looming, the Delta variant is posing a threat to that view. The [pace of the recovery](https://www.cnn.com/2021/07/19/economy/recession-end-covid-nber/index.html) has been moderating since the spring. Come Thursday, a first look at second-quarter gross domestic product growth — the broadest measure of economic activity — will show what the summer lull really means. Economists polled by Refinitiv expect GDP has grown at an annualized pace of 8.5% between April and June, which would be the [biggest advance since](https://fred.stlouisfed.org/series/A191RL1Q225SBEA) the third quarter last year, when the [economy roared back](https://www.cnn.com/2020/10/29/economy/gdp-report-third-quarter/index.html) following a [sharp contraction](https://www.cnn.com/2020/07/30/economy/us-economy-2020-second-quarter/index.html). Citi economist Veronica Clark attributes the predicted Q2 strength to rampant consumer spending on goods and services. Consumption of goods rose even further above the spring's pre-pandemic level thanks to the effects of Washington's stimulus checks. "Spending on many services, such as dining at restaurants, returned to pre-Covid levels by the end of Q2," Clark said in a note to clients, but there's room for further to improvement in the second half of this year, Clark said in a note to clients. Not yet back to normal Yet the road to recovery has become more challenging in the weeks since the second quarter. The [Back-to-Normal index](https://www.cnn.com/business/us-economic-recovery-coronavirus) created by CNN Business and Moody's Analytics has been static over the past few weeks. At 92% back to its pre-pandemic strength, the economy [still has a little further to go in making up ground.](https://www.cnn.com/2021/06/20/investing/stocks-week-ahead/index.html) While the July 4 and Labor Day holidays skew the index a little, the summer recovery lull might be due to other factors, said Moody's Analytics associate economist Matt Colyar. The next few weeks will be telling. "Though it's hard to tease out in the data just yet, I primarily attribute the potential slowdown to the Delta spread," he told CNN Business in an email. For example, business confidence "was on a tear in May and June," Colyar said, but the renewed rise in infections has put that momentum in jeopardy. "No one seems to think sweeping restrictions are coming back, but the softness in the [business confidence] survey feels like the 'dangerous variant' fears [are] being realized." This distinction is important: A full lockdown of the sort we saw in the pandemic's earliest days is unlikely to repeat itself. But some infection-preventing measures could reappear, and people might start being more cautious again. On Tuesday the US Centers for Disease Control and Prevention [updated its coronavirus guidelines](https://www.cnn.com/2021/07/27/health/cdc-mask-guidance-vaccinated-people-bn/index.html), recommending masks for vaccinated people in areas with high or substantial transmission of the virus. This applies to nearly two-thirds of all US counties. But urging people to wear masks again is unlikely to unravel the economic recovery, Colyar said. Rather, it could be a drag on the pace of improvements going forward, particularly in comparison to the spring or last summer.

### 1ar – ! – economy

#### Countries turn inward---prefer post-COVID evidence.

Walt 20, Robert and Renée Belfer professor of international relations at Harvard University. (Stephen M., 5/13/20, “Will a Global Depression Trigger Another World War?”, *Foreign Policy*, https://foreignpolicy.com/2020/05/13/coronavirus-pandemic-depression-economy-world-war/)

One familiar argument is the so-called diversionary (or “scapegoat”) theory of war. It suggests that leaders who are worried about their popularity at home will try to divert attention from their failures by provoking a crisis with a foreign power and maybe even using force against it. Drawing on this logic, some Americans now worry that President Donald Trump will decide to attack a country like Iran or Venezuela in the run-up to the presidential election and especially if he thinks he’s likely to lose.

This outcome strikes me as unlikely, even if one ignores the logical and empirical flaws in the theory itself. War is always a gamble, and should things go badly—even a little bit—it would hammer the last nail in the coffin of Trump’s declining fortunes. Moreover, none of the countries Trump might consider going after pose an imminent threat to U.S. security, and even his staunchest supporters may wonder why he is wasting time and money going after Iran or Venezuela at a moment when thousands of Americans are dying preventable deaths at home. Even a successful military action won’t put Americans back to work, create the sort of testing-and-tracing regime that competent governments around the world have been able to implement already, or hasten the development of a vaccine. The same logic is likely to guide the decisions of other world leaders too.

Another familiar folk theory is “military Keynesianism.” War generates a lot of economic demand, and it can sometimes lift depressed economies out of the doldrums and back toward prosperity and full employment. The obvious case in point here is World War II, which did help the U.S economy finally escape the quicksand of the Great Depression. Those who are convinced that great powers go to war primarily to keep Big Business (or the arms industry) happy are naturally drawn to this sort of argument, and they might worry that governments looking at bleak economic forecasts will try to restart their economies through some sort of military adventure.

I doubt it. It takes a really big war to generate a significant stimulus, and it is hard to imagine any country launching a large-scale war—with all its attendant risks—at a moment when debt levels are already soaring.

More importantly, there are lots of easier and more direct ways to stimulate the economy—infrastructure spending, unemployment insurance, even “helicopter payments”—and launching a war has to be one of the least efficient methods available. The threat of war usually spooks investors too, which any politician with their eye on the stock market would be loath to do.

Economic downturns can encourage war in some special circumstances, especially when a war would enable a country facing severe hardships to capture something of immediate and significant value. Saddam Hussein’s decision to seize Kuwait in 1990 fits this model perfectly: The Iraqi economy was in terrible shape after its long war with Iran; unemployment was threatening Saddam’s domestic position; Kuwait’s vast oil riches were a considerable prize; and seizing the lightly armed emirate was exceedingly easy to do. Iraq also owed Kuwait a lot of money, and a hostile takeover by Baghdad would wipe those debts off the books overnight. In this case, Iraq’s parlous economic condition clearly made war more likely. Yet I cannot think of any country in similar circumstances today. Now is hardly the time for Russia to try to grab more of Ukraine—if it even wanted to—or for China to make a play for Taiwan, because the costs of doing so would clearly outweigh the economic benefits. Even conquering an oil-rich country—the sort of greedy acquisitiveness that Trump occasionally hints at—doesn’t look attractive when there’s a vast glut on the market. I might be worried if some weak and defenseless country somehow came to possess the entire global stock of a successful coronavirus vaccine, but that scenario is not even remotely possible.