## 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/#_ftn10) Shortly after these events, President Trump issued Executive Order 13920, “[Securing the United States Bulk-Power System](https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/),” essentially limiting the import of Chinese-built critical energy infrastructure components due to concerns about cybersecurity.[[11]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn11) Interestingly, Jiangsu Huapeng “boasted that it supported 10 percent of New York City’s electricity load.”[[12]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn12)

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

#### Those attacks cause accidental nuclear escalation.

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

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

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

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

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

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

The Nuclear-Cyber Connection

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

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

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

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

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

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

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

Pathways to Escalation

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

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

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

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

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

### 1AC---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 – at: K

### 2ac – perm

#### Permutation do both combines the aff’s riskification with the alt’s critical stance on hyperbolic threat inflation---the net benefit is avoiding blanket desecuritization that cedes political terrain to the surveillance industrial complex.

Friis et al. 16, \*Karsten Friis and Erik Reichborn-Kjennerud, Norwegian Institute of International Affairs (NUPI) (“From Cyber Threats to Cyber Risks”, Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives, Karsten Friis and   
Jens Ringsmose eds., London: Routledge, 2016)

However, a focus on risk also means attention to vulnerabilities. This can have positive and negative effects. One could argue that looking at vulnerabilities instead of at external actors can result in an unhealthy focus on worst-case catastrophes – which again may lead to increased militarisation of cyberspace (Cavelty 2012). On the other hand, such a focus may lead to an effort to reduce vulnerabilities, thus minimising certain risks, such as systemic failures and cyber crime. In addition, a focus on vulnerabilities rather than actors may have the benefit of cyber security not becoming a self-fulfilling prophecy of a new Cyber Cold War. We will conclude this chapter with further ethical considerations regarding the impact of our theoretical approach.

Conclusion

The inherent normative approach of the Copenhagen School is that securitization may often not be a good thing: 'security should be seen as negative, as a failure to deal with issues as normal politics' (Buzan et al. 1998). De-securitization, in other words a return to normal politics with less dramatic features, is therefore often seen as desirable. This particularly applies to sectors like human security or environmental security, where state-centric and militarised solutions may exacerbate rather than reduce tensions (Hansen 2012). As we argued at the outset of this chapter, the same can be said about cyber security. Attempts at securitization have placed part of the cyber debate, particularly in the USA, in the military logic of friend and foe, deterrence and war. This may also have 'legitimised' some of the intrusive privacy practices of the NSA, as revealed by Edward Snowden.

However, Corry warns that de-securitization may also have negative effects. In the case of climate change, it could lead to 'de-riskification', thus 'removing climate change away from this precautionary logic and into ‘normal' politics of distribution of goods and bads' (Corry 2012, 255). This is where climate sceptics would like to see the debate; in other words as entirely decoupled from security and heightened political attention. For others, climate change is something that requires particular attention and preparedness, as it is on a higher policy level than day-to-day politics.

In the cyber domain, few voices seek to reject the risks altogether, but the normative imperative of talking in terms of risk rather than threats de-escalates the discourse. If that were to fail, cyber security would become a domain totally dominated by security and intelligence agencies, technical experts and not least the booming 'cyber-security military- industrial complex' that simultaneously cries wolf and offers solutions (Deibert 2013).

Riskification is thus an analytical tool that can be applied in order to empirically capture cyber security efforts, the representation of the danger and the policies formulated to address it, as well as a way to conduct critical analysis aimed at unmasking securitization efforts in this field. Empirical analysis will most likely find that the riskification in certain places and at certain times begins to resemble securitization. As with climate change, such securitization of cyber can be criticised while offering an alternative security frame, so that a return to normal politics no longer is the only option.

Nonetheless, following a Foucauldian approach to risk, one may argue that risk policies are as dangerous to the freedom of society as securitization and militarisation, since the former represent a more creeping and gradual change to the security and control measures of neo- liberal regimes of power that call for a permanent process with no end. The slow processes normalise security policies that would arguably have met resistance had they been put in place abruptly. From this perspective, replacing securitization with riskification may not be a positive move if the valued referent object is a free and transparent cyberspace.

Applying riskification analytically therefore does not need to automatically correspond to advocating riskification of cyber security politically. That is a value judgement. Riskification as an analytical tool can be applied without taking a normative stance on these matters, but it can also be applied as a platform for critical judgements of current policies.

As we see it, applying riskification to the study of cyber security has important benefits. It allows analysts to capture processes that may be at the boundary between risk and threat, perhaps not existential, but still grave. It further allows escalation and de-escalation within the same basic analytical parameters, and can also be combined with some of the proposed 'new grammars' of the Copenhagen School discussed here, such as 'technification'. Importantly, it allows for a deeper understanding of the intended and unintended material aspects of and the role of cyber security professionals in production of cyber security. Furthermore, riskification does not preclude the continued use of other theoretical tools like 'frame analysis' and 'agenda setting-theory'. It helps us escape the hyperbolic language of threats and dangers while remaining seriously committed to recognising and understanding the risks and vulnerabilities of our networked societies. It may also serve as a normative platform for the defence of internet freedom against the growing pressure from the intelligence services and the surveillance industry towards increased control and surveillance. With a less dramatic representation of the cyber dangers, legitimate countermeasures will most likely be less intrusive and omnipotent.

#### Permutation do the aff then the alternative in all other instances.

### 2AC---AT: IR K---China

#### Western IR explains China’s behavior---suggesting otherwise ignores centuries of Chinese history.

Chong 20, PhD, associate professor of political science at the National University of Singapore and a Harvard-Yenching Institute Visiting Scholar for 2019-2020. (Ja Ian, 11/9/20, "Roundtable 12-2 on *Thucydides’s Trap? Historical Interpretation, Logic of Inquiry, and the Future of Sino-American Relations*", *H-Diplo | ISSF*, https://issforum.org/roundtables/12-2-thucydides)

Chan’s finding that misplaced worries about the PRC and its intentions stem in part from misunderstandings of perspectives on international politics that are informed by theories from “the West” rather than China deserves elaboration and debate. So-called “Western” international relations theories often have parallels in the Chinese tradition, broadly construed. Work analyzing Spring and Autumn, Warring States, Song, and Ming documents indicate that the strategic thought that is prominent in these periods closely resembles statecraft familiar to those in the contemporary “West.”[16] Texts as varied as the Han-era annals Records of the Grand Historian and the Ming-era fiction Romance of the Three Kingdoms will suggest the same.[17] Parallels between “Western” and “Chinese” approaches to politics are unsurprising. Several millennia of collective human experience, thought, and debate over statecraft, conflict, as well as governance are almost certainly bound to produce similarities in responses.

Dividing the world into “Western” and “Chinese” views of the world ignores the fact the PRC has disagreements with ostensibly “non-Western” polities such as India, Indonesia, Japan, Korea, and Vietnam, each with their own distinct philosophical traditions.[18] Also, despite sharing cultural origins, people in the PRC and on Taiwan disagree fundamentally issues of political valAues and rights, not the relatively simple issues of who should rule China or what a Chinese state should entail geographically.[19] Moreover, the PRC’s ruling Chinese Communist Party draws at least some of its inspiration from European thinkers in the form of Karl Marx and Vladimir Lenin. Successive dynasties from historical China also proved themselves very adept at conquest—that is how regimes and empires get built.[20] Attributing tensions between the United States and PRC to culture suggests an overly monolithic view of the rich and varied philosophical and political traditions both major powers draw from, giving them less credit than is due.[21]

To claim that contemporary international scholarship and U.S. policy are unable to adequately understand China because they are “Western” may oversimplify the nature and seriousness of problems dogging U.S.-China relations and their consequences for the world. Relegating difference to culture is not only Orientalizing, it can encourage a misplaced expectation that understanding can bring some sort of happy, mutually acceptable outcome. Perhaps Beijing and Washington understand each other well. They simply disagree fundamentally over values and interests in ways that make finding mutually acceptable accommodation increasingly difficult. This does not have to imply that either side is morally superior or normatively “better” than the other, just that understanding provides little promise for improving relations and avoiding confrontation. Better accounting for such possibilities invites fuller consideration of the roles that agency and contingency play in major power relations, two features that Chan clearly identifies as critical in the volume.

### 2AC---Impact Framing

#### Weigh impacts using expected value, or magnitude times probability---it’s the only to ethically account for the underappreciated risk of high-magnitude threats.

Harris 17, \*John Harris is Politico’s editor-in-chief and author of The Survivor: Bill Clinton in the White House; \*Bryan Bender is Politico’s national security editor and author of You Are Not Forgotten. Both Harris and Bender covered the Pentagon during the tenure of Secretary of Defense William J. Perry; (January 6th, 2017, “Bill Perry Is Terrified. Why Aren’t You?”, https://www.politico.com/magazine/story/2017/01/william-perry-nuclear-weapons-proliferation-214604/)

And there’s one other difference from the Cold War: Americans no longer think about the threat every day.

Nuclear war isn’t the subtext of popular movies, or novels; disarmament has fallen far from the top of the policy priority list. The largest upcoming generation, the millennials, were raised in a time when the problem felt largely solved, and it’s easy for them to imagine it’s still quietly fading into history. The problem is, it’s no longer fading. “Today, the danger of some sort of a nuclear catastrophe is greater than it was during the Cold War,” Perry said in an interview in his Stanford office, “and most people are blissfully unaware of this danger.”

It is a turn of events that has an old man newly obsessed with a question: Why isn’t everyone as terrified as he is?

Perry’s hypothesis for the disconnect is that much of the population, especially that rising portion with no clear memories of the first Cold War, is suffering from a deficit of comprehension. Even a single nuclear explosion in a major city would represent an abrupt and possibly irreversible turn in modern life, upending the global economy, forcing every open society to suspend traditional liberties and remake itself into a security state. “The political, economic and social consequences are beyond what people understand,” Perry says. And yet many people place this scenario in roughly the same category as the meteor strike that supposedly wiped out the dinosaurs—frightening, to be sure, but something of an abstraction.

So Perry regards his last great contribution of a 65-year career as a crusade to stimulate the public imagination—to share the vivid details of his own nightmares. He is doing so in a recent memoir, in a busy public speaking schedule, in half-empty hearing rooms on Capitol Hill, and increasingly with an online presence aimed especially at young people. He has enlisted the help of his 28-year-old granddaughter to figure out how to engage a new generation, including [through a series of virtual lectures](https://lagunita.stanford.edu/courses/course-v1:Engineering+NuclearBrink+Fall2016/about) known as a MOOC, or massive open online course. He is eagerly signing up for “Ask Me Anything” chats on Reddit, in which some people still confuse him with William “The Refrigerator” Perry of NFL fame. He posts his ruminations on YouTube, where they give Katy Perry no run for her money, even as the most popular are closing in on 100,000 views. One of the nightmare scenarios Perry invokes most often is designed to roust policymakers who live and work in the nation’s capital. The terrorists would need enriched uranium. Due to the elaborate and highly industrial nature of production, hard to conceal from surveillance, fissile material is still hard to come by—but, alas, far from impossible. Once it is procured, with help from conspirators in a poorly secured overseas commercial power centrifuge facility, the rest of the plot as Perry imagines it is no great technological or logistical feat. The mechanics of building a crude nuclear device are easily within the reach of well-educated and well-funded militants. The crate would arrive at Dulles International Airport, disguised as agricultural freight. The truck bomb that detonates on Pennsylvania Avenue between the White House and Capitol instantly kills the president, vice president, House speaker, and 80,000 others. Where exactly is your office? Your house? And then, as Perry spins it forward, how credible would you find the warnings, soon delivered to news networks, that five more bombs are set to explode in unnamed U.S. cities, once a week for the next month, unless all U.S. military personnel overseas are withdrawn immediately? If this particular scenario does not resonate with you, Perry can easily rattle off a long roster of others—a regional war that escalates into a nuclear exchange, a miscalculation between Moscow and Washington, a computer glitch at the exact wrong moment. They are all ilks of the same theme—the dimly understood threat that the science of the 20th century is set to collide with the destructive passions of the 21st. “We’re going back to the kind of dangers we had during the Cold War,” Perry said. “I really thought in 1990, 1991, 1992, that we left those behind us. We’re starting to re-invent them. We and the Russians and others don’t understand that what we’re doing is re-creating those dangers—or maybe they don’t remember the dangers. For younger people, they didn’t live through those dangers. But when you live through a Cuban Missile Crisis up close and you live through a false alarm up close, you do understand how dangerous it is, and you believe you should do everything you could possibly do to [avoid] going back.” For people who follow the national security priesthood, the dire scenarios are all the more alarming for who is delivering them. Through his long years in government Perry invariably impressed colleagues as the calmest person in the room, relentlessly rational, such that people who did not know him well—his love of music and literature and travel—regarded his as a purely analytical mind, emotion subordinated to logic and duty. Starting in the 1950s as a technology executive and entrepreneur in some of the most secretive precincts of the defense industry, he gradually took on a series of high-level government assignments that gave him one of the most quietly influential careers of the Cold War and its aftermath. Fifteen years before serving as Bill Clinton’s secretary of defense, Perry was the Pentagon official in charge of weapons research during the Carter administration. It was from this perch that he may have had his most far-reaching impact, and left him in some circles as a legendary figure. He used his office to give an essential push to two ideas that transformed warfare over the next generation decisively to American advantage. One idea was stealth technology, which allowed U.S. warplanes to fly over enemy territory undetected. The other was precision-guided munitions, which allowed U.S. bombs to land with near-perfect accuracy. During the Clinton years, Perry so prized his privacy that he initially turned down the job of Defense secretary—changing his mind only after Clinton and Al Gore pleaded with him that the news media scrutiny wouldn’t be so bad. The reputation he built over a life in the public sphere is starkly at odds with this latest highly impassioned chapter of Perry’s career. Harold Brown, who also is 89, first recruited Perry into government, and was Perry’s boss while serving as Defense secretary in the Carter years. “No one would have thought of Bill Perry as a crusader,” he says. “But he is on a crusade.” Lee Perry, his wife of nearly 70 years, is living in an elder care facility, her once buoyant presence now lost to dementia. Perry himself, lucid as ever, has seen his physical frame become frail and stooped. Rather than slowing his schedule, he has accelerated his travels to plead with people to awaken to the danger. A trip to Washington includes a dinner with national security reporters and testimony on Capitol Hill. Back home in California, he’s at the Google campus to prod engineers to contemplate that their world may not last long enough for their dreams of technology riches to come true. He’s created an advocacy group, [the William J. Perry project](http://www.wjperryproject.org/), devoted to public education about nuclear weapons. He’s enlisted both his granddaughter and his 64-year-old daughter, Robin Perry, in the cause. But if his profile is rising, his style is essentially unchanged. He is a man known for self-effacement, trying to shape an era known for relentless self-promotion, a voice of quiet precision in a time of devil-take-the-hindmost bombast. The rational approach to problem-solving that propelled his career and won him adherents and friends in both political parties and even among some of America’s erstwhile enemies remains his guide—in this case, by endeavoring to calculate the possibilities and probabilities of a terrorist attack, regional nuclear war, or horrible miscalculation with Russia. “I want to be very clear,” he said. “I do not think it is a probability this year or next year or anytime in the foreseeable future. But the consequence is so great, we have to take it seriously. And there are things to greatly lower those possibilities that we’re simply not doing.” \*\*\* Perry really did not expect he would have to write this chapter of his public life. His official career closed with what seemed then an unambiguous sense of mission accomplished. By the time he arrived in the Pentagon’s top job in 1994, the Cold War was over, and the main item on the nuclear agenda seemed to be cleaning up no-longer-needed arsenals. As defense secretary, Perry stood with his Russian counterpart, Pavel Grachev, as they jointly blew up missile silos in the former Soviet Union and tilled sunflower seeds in the dirt. “I finally thought by the end of the ‘80s we lived through this horrible experience and it’s behind us,” Perry said. “When I was secretary, I fully believed it was behind us.” After leaving the Pentagon, he accepted an assignment from Clinton to negotiate an end to North Korea’s nuclear development program—and seemed agonizingly close to a breakthrough as the last days of the president’s term expired. Now, he sees his grandchildren inheriting a planet possibly more dangerous than it was during his public career. No one could doubt that the Sept. 11 terrorists would have gladly used nuclear bombs instead of airplanes if they had had them, and it seems only a matter of time until they try. Instead of a retreating threat in North Korea, that fanatical regime now possesses as many as eight nuclear bombs, and is just one member of a growing nuclear club. Far from a new partnership with Russia, Vladimir Putin has given old antagonisms a malevolent new face. American policymakers talk of spending up to $1 trillion to modernize the nuclear arsenal. And now comes Donald Trump with a long trail of statements effectively shrugging his shoulders about a world newly bristling with bombs and people with reasons to use them. Perry knew Hillary Clinton well professionally, and says he admired both her and Bill Clinton for their professional judgment though he was never a personal intimate of either. He was prescient before the election in expressing skepticism about how voters would respond to the dynastic premise of the Clinton campaign—a healthy democracy should grow new voices—but was as surprised as everyone else on Election Day. Donald Trump was not the voice he was looking for, to put it mildly, but he has responded to the Trump cyclone with modulated restraint. Perry said he assumes his most truculent rhetoric isn’t serious, the utterances of a man who assumed his words were for political effect only and had no real consequences. Now that they do, Perry is hoping to serve as a kind of ambassador to rationality. He said he is hoping for audiences soon, with Trump if the incoming president will see him, and certainly Trump’s national security team, which includes several people Perry knows, including Defense Secretary nominee James Mattis. There is little doubt the message if the meeting comes. “We are starting a new Cold War,” he says. “We seem to be sleepwalking into this new nuclear arms race. … We and the Russians and others don’t understand what we are doing.” “I am not suggesting that this Cold War and this arms race is identical to the old one,” Perry added. “But in many ways, it is just as bad, just as dangerous. And totally unnecessary.” \*\*\* Perry had been brooding over the question for a year. It was in the early 1950s, he was still in his 20s, and the subject was partial differential equations—the topic of his Ph.D. thesis. A particular problem had been absorbing him, day in and day out, hours and hours on end. Then, out of nowhere, a light came on. Math for Perry represented analytical discipline, a way of achieving mastery not only over numerical problems but any hard problem, by breaking it down into essential parts, distilling complexity into simplicity. | Photo via the William J. Perry Project “I woke up in the middle of the night, and it was all there,” Perry recalled. “It was all there, and I got out of bed and sat down. The next two or three hours, I wrote my thesis, and from the first word I wrote down, I never doubted what the last word was going to be: It was a magic moment.” The story is a reminder of something definitional about Bill Perry. Before he became in recent years an apostle of disarmament, before he sat atop the nation’s war-making apparatus in the 1990s, before he was the executive of a defense contractor specializing in the most complex arenas of Cold War surveillance in the 1960s, he was a young man in love with mathematics. In those days, Perry had planned on a career as a math professor. His attraction to math was not merely practical, in the way that engineers or architects rely on math. The appeal was just as much aesthetic, in ways that people who are not numbers people—political life tends to be dominated by word people—cannot easily comprehend. To Perry’s mind, there was a purity to math, a beauty to the patterns and relationships, that was not unlike music. Math for Perry represented analytical discipline, a way of achieving mastery not only over numerical problems but any hard problem, by breaking it down into essential parts, distilling complexity into simplicity. This trait was why Pentagon reporters in the 1990s liked spending time around Perry. When most public officials are asked a question, one studies the transcript later to decipher a succession of starts and stalls, sentence fragments and ellipses, that cumulatively convey an impressionistic sense of mind but no clear fixed meaning. Perry’s sentences, by contrast, always cut with surgical precision. It was one reason Clinton White House officials often held their breath when he gave interviews—Perry might make news by being clear on subjects, such as ethnic warfare in the Balkans or a nuclear showdown in North Korea, that the West Wing preferred to try to fog over.

“I’ve never been able to attack a policy problem with a mathematical formula,” he recalled, “but I have always believed that the rigorous way of thinking about a problem was good. It separated the fact from the bullshit, and that’s very important sometimes, to separate what you can from what you would hope you can do.”

Just how high is the risk? The answer is ultimately unknowable. Perry’s point, though, is that it’s a hell of a lot higher than you think. | M. Scott Mahaskey/POLITICO

Perry wishes more people were familiar with the concept of “expected value.” That is a statistical way of understanding events of very large magnitude that have a low probability. The large magnitude event could be something good, like winning a lottery ticket. Or it could be something bad, like a nuclear bomb exploding. Because the odds of winning the lottery are so low, the rational thing is to save your money and not buy the ticket. As for a nuclear explosion, by Perry’s lights, the consequences are so grave that the rational thing would be for people in the United States and everywhere to be in a state of peak alarm about their vulnerability, and for political debate to be dominated by discussion of how to reduce the risk.

And just how high is the risk? The answer of course is ultimately unknowable. Perry’s point, though, is that it’s a hell of a lot higher than you think.

Perry invites his listeners to consider all the various scenarios that might lead to a nuclear event. “Mathematically speaking, you add those all together in one year it is still just a possibility, not a probability,” he reckons. “But then you go out ten, twenty years and each time this possibility repeats itself, and then it starts to become a probability. How much time we have to get those possibility numbers lower, I don’t know. But sooner or later the odds are going to get us, I am afraid.”

\*\*\*

Almost uniquely among living Americans, Bill Perry has actually faced down the prospect of nuclear war before—twice. In the fall of 1962, Bill Perry was 35, father of five young children, living in the Bay Area and serving as director of Sylvania’s Electronic Defense Laboratories—driving his station wagon to recitals in between studying missile trajectories and the radius of nuclear detonations. Where he resided was not then called Silicon Valley, but the exuberance and spirit of creative possibility we now associate with the region was already evident. The giants then were Bill Hewlett and David Packard, men Perry deeply admired and wished to emulate in his own business career. The innovation engine at that time, however, was not consumer technology; it was the government’s appetite for advantage in a mortal struggle against a powerful Soviet foe. Perry was known as a star in the highly complex field of weapons surveillance and interpretation. So it was not a surprise, one bright October day, for Perry to get a call from Albert “Bud” Wheelon, a friend at the Central Intelligence Agency. Wheelon said he wanted Perry in Washington for a consultation. Perry said he’d juggle his schedule and be there the next week. “No,” Wheelon responded. “I need to see you right away.” Perry caught the red-eye from San Francisco, and went straight to the CIA, where he was handed photographs whose meaning was instantly clear to him. They were of Soviet missiles stationed in Cuba. For the next couple weeks, Perry would stay up past midnight each evening poring over the latest reconnaissance photos and help write the analysis that senior officials would present the next morning to President Kennedy. Perry experienced the crisis partly as ordinary citizen, hearing Kennedy on television draw an unambiguous line against Soviet missiles in this hemisphere and promising that any attack would be met with “a full retaliatory response.” But he possessed context, about the capabilities of weapons and the daily state of play in the crisis, that gave him a vantage point superior to that of all but perhaps a few dozen people. “I was part of a small team—six or eight people,” he recounted of those days 54 years earlier. “Half of them technical experts, half of them intelligence analysts, or photo interpreters. It was a minor role but I was seeing all the information coming in. I thought every day when I went back to the hotel it was the last day of my life because I knew exactly what nuclear weapons could do. I knew it was not just a lot of people getting killed. It was the end of civilization and I thought it was about to happen.” Left: A January 1963 aerial photo showing that the Soviets had disbanded medium- and intermediate-range ballistic missile sites in Cuba. Right: Soviet freighter Polzunov (top) loaded with nuclear missiles removed from Cuba, is escorted by American destroyer Vesole outside Cuban waters on trek back to Russia near end of Cuban Missile Crisis. | Defense Department; Carl Mydans/The LIFE Picture Collection/Getty Images It was years later that Perry, like other more senior participants in the crisis, learned how right that appraisal was. Nuclear bombs weren’t only heading toward Cuba on Soviet ships, as Kennedy believed and announced to Americans at the time. Some of them were already there, and local commanders had been given authority to use them if Americans launched a preemptive raid on Cuba, as Kennedy was being urged, goaded even, by Air Force Gen. Curtis LeMay and other military commanders. At the same time, Soviet submarines were armed and one commander had been on the verge of launching them until other officers on the vessel talked him out of it. Either event would have in turn sent U.S. missiles flying. The Cuban Missile Crisis recounting is one of the dramatic peaks in “My Journey on the Nuclear Brink,” the memoir Perry published last fall. It is a book laced with other close calls—like November 9, 1979, when Perry was awakened in the middle of the night by a watch officer at the North American Aerospace and Defense Command (NORAD) reporting that his computers showed 200 Soviet missiles in flight toward the United States. For a frozen moment, Perry thought: This is it—This is how it ends. The watch officer soon set him at ease. It was a computer error, and he was calling to see whether Perry, the technology expert, had any explanation. It took a couple days to discover the low-tech answer: Someone had carelessly left a crisis-simulation training tape in the computer. All was well. But what if this blunder had happened in the middle of a real crisis, with leaders in Washington and Moscow already on high alert? The inescapable conclusion was the same as it was in 1962: The world skirting nuclear Armageddon as much by good luck as by skilled crisis management. Perry is part of a distinct cohort in American history, one that didn’t come home with the large-living ethos of the World War II generation, but took responsibility for cleaning up the world that the war bequeathed. He was a 14-year-old in Butler, Pennsylvania when he heard the news of the Pearl Harbor attack in a friend’s living room, and had the disappointed realization that the war might be over by the time he was old enough to fight in it. That turned out to be true—he was just shy of 18 at war’s end—a fact that places Perry in what demographers have called the “Silent Generation,” too young for one war but already middle-aged by the time college campuses erupted over Vietnam. Like many in his generation, Perry was not so much silent as deeply dutiful, with an understated style that served as a genial, dry-witted exterior to a life in which success was defined by how faithfully one met his responsibilities. Perry said he became aware, first gradually and over time profoundly, of the surreal contradictions of his professional life. His work—first at Sylvania and then at ESL, a highly successful defense contracting firm he co-founded in 1963—was relentlessly logical, analyzing Soviet threats and intentions and coming up with rational responses to deter them. But each rational move was part of a supremely irrational dynamic—“mutually assured destruction”—that placed the threat of massive casualties at the heart of America’s basic strategic thinking. It was the kind of framework in which policymakers could accept that a mere 25 million people dead was good news. Also the kind that in one year alone led the United States to produce 8,000 nuclear bombs. By the end, the Cold War left the planet with about 70,000 bombs ([a total that](https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat) is now down to about 15,500). “I think probably everybody who was involved in nuclear weapons in those days would see the two sides of it,” Perry recalls, “the logic of deterrence and the madness of deterrence, and there was no mistake, I think, that the acronym was MAD.” \*\*\* Perry has been at the forefront of a movement that he considers the sane and only alternative, and he has joined forces with other leading Cold Warriors who in another era would likely have derided their vision as naïve. In January 2007, he was a co-author of a remarkable commentary that ran on the op-ed page of the Wall Street Journal. It was signed also by two former secretaries of state, George Schulz and Henry Kissinger and by Sam Nunn, a former chairman of the Senate Armed Services Committee—all leading military hawks and foreign policy realists who came together to argue for something radical: that the goal of U.S. policy should be not merely the reduction and control of atomic arms, it should be the ultimate elimination of all nuclear weapons. This sounded like gauzy utopianism, especially bizarre coming from supremely pragmatic men. But Perry and the others always made clear they were describing a long-term ideal, one that would only be achieved through a series of more incremental steps. The vision was stirring enough that it was endorsed by President Obama in his opening weeks in office, in a March 2009 address in Prague. In retrospect, Obama’s speech may have been the high point for the vision of abolition. “A huge amount of progress was made,” recalled Shultz, now 93. “Now it is going in the other direction.” “We have less danger of an all-out war with Russia,” in Nunn’s view. “But we have more danger of some type of accident, miscalculation, cyber interference, a terrorist group getting a nuclear weapon. It requires a lot more attention than world leaders are giving it.” Perry’s goal now is much more defensive than it was just a few years ago—halting what has become inexorable momentum toward reviving Cold War assumptions about the central role of nukes in national security. More recently he’s added yet another recruit to his cause: California Governor Jerry Brown. Brown, now 78, met Perry a year ago, after deciding that he wanted to devote his remaining time in public service mainly to what he sees as civilization’s two existential issues, climate change and nuclear weapons. Brown said he became fixated on spreading Perry’s message after reading his memoir: He recently gave a copy to President Obama and is trying to bend the ear of others with influence in Washington. If Bill Perry has a gift for understatement, Brown has a gift for the theatrical. In an interview at the governor’s mansion in Sacramento, he wonders why everyone is not paying attention to his new friend and his warnings for mankind. “He is at the brink! At the brink! Not WAS at the brink—IS at the brink,” Brown exclaimed. “But no one else is.” A California governor can have more influence, at least indirectly, than one might think, due to the state’s outsized role in policy debates and the fact that the University of California’s Board of Regents helps manage some of the nation’s top weapons laboratories, which study and design nuclear weapons. Brown, who was a vocal critic in the 1980s of what he called America's "nuclear addiction," reviewed Perry's recent memoir in the New York Review of Books, and said he is determined to help his new friend spread his message. “Everybody is, 'we are not at the brink,' and we have this guy Perry who says we are. It is the thesis that is being ignored." Even if more influential people wake up to Perry’s message—a nuclear event is more likely and will be more terrible than you realize—a hard questions remains: Now what? This is where Perry’s pragmatism comes back into play. The smartest move, he thinks, is to eliminate the riskiest part of the system. If we can’t eliminate all nukes, Perry argues, we could at least eliminate one leg of the so-called nuclear triad, intercontinental ballistic missiles. These are especially prone to an accidental nuclear war, if they are launched by accident or due to miscalculation by a leader operating with only minutes to spare. Nuclear weapons carried by submarines beneath the sea or aboard bomber planes, he argues, are logically more than enough to deter Russia.

The problem, he knows, is that logic is not necessarily the prevailing force in political debates. Psychology is, and this seems to be dictating not merely that we deter a Russian military force that is modernizing its weapons but that we have a force that is self-evidently superior to them.

It is an argument that strikes Perry as drearily familiar to the old days. Which leads him the conclusion that the only long-term way out is to persuade a younger generation to make a different choice.

His granddaughter, Lisa Perry, is precisely in the cohort he needs to reach. At first she had some uncomfortable news for her grandfather: Not many in her generation thought much about the issue.

“The more I learned from him about nuclear weapons the more concerned I was that my generation had this massive and dangerous blind spot in our understanding of the world,” she said in an interview. “Nuclear weapons are the biggest public health issue I can think of.”

But she has not lost hope that their efforts can make a difference, and today she has put her graduate studies in public health on hold to work full time for the Perry Project as its social media and web manager. “It can be easy to get discouraged about being able to do anything to change our course,” she said. “But the good news is that nuclear weapons are actually something that we as humans can control...but first we need to start the conversation.”

It was with her help that Perry went on Reddit to [field questions](https://www.reddit.com/r/IAmA/comments/4a0ga4/iam_william_j_perry_former_secretary_of_defense/) ranging from how his PhD in mathematics prepared him to what young people need to understand.

“As a 90s baby I never lived in the Cold War era,” wrote one participant, with the Reddit username BobinForApples. “What is one thing today's generations will never understand about life during the Cold War?”

Perry answered, as SecDef19: “Because you were born in the 1990s, you did not experience the daily terror of ‘duck and cover’ drills as my children did. Therefore the appropriate fear of nuclear weapons is not part of your heritage, but the danger is just as real now as it was then. It will be up to your generation to develop the policies to deal with the deadly nuclear legacy that is still very much with us.”

For the former defense secretary, the task now is to finally—belatedly—prove Einstein wrong. The physicist said in 1946: “The unleashed power of the atom has changed everything save our modes of thinking and we thus drift toward unparalleled catastrophe.”

In Perry’s view the only way to avoid it is by directly contemplating catastrophe—and doing so face to face with the world’s largest nuclear power, Russia, as he recently did in a forum in Luxembourg with several like-minded Russians he says are brave enough to speak out about nuclear dangers in the era of Putin.

#### Extinction outweighs---our framing shifts security policy from a national to existential frame---solves their threat K’s.

Sears 20, \*Nathan Sears, PhD Candidate in Political Science at The University of Toronto and Trudeau Fellow in Peace, Conflict and Justice at the Munk School of Global Affairs (April 17th, 2020, “Existential Security: Towards a Security Framework for the Survival of Humanity,” https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.12800)

‘Existential security’ responds to a similar set of questions as alternative security frames (see Table 2). Security for whom? The ‘referent object’ of existential security is humanity. Security is therefore about humanity’s survival . Security for which values? The ‘values’ to be secured are, at the minimum, the survival of humanity (i.e. the biological entity of the human species and cultural entity of human civilization), and, at the maximum, the long‐term prosperity of human civilization and the planet. The security of humankind ranges from the survival of existing human beings and societies to past and future generations of humanity – the past whose memory is recorded in history and preserved by the present, and the future whose possibilities of existence depend on actions taken in the present. Existential security therefore adopts an intergenerational perspective of security, not only for utilitarian reasons (e.g. quantifying the potential gains/losses in ‘future lives’) (Baum, 2015; Bostrom, 2002, 2013; Torres, 2017), but also because the significance of humankind – that is, all its past sufferings, present achievements, and future potential – is at stake, since existential risks simultaneously threaten humanity’s past, present, and future (Morgenthau, 1961).

How much security? Nick Bostrom (2013, p. 19) proposes the principle of ‘maxipok’, in which security policy would seek to ‘maximise the probability of an “OK outcome”, where an OK outcome is any outcome that avoids existential catastrophe’. While reducing the probability of existential risk to ‘zero’ may be impossible, the amount of security should be determined by a level of risk‐aversion equivalent to existential threats. Since thinking in terms of ‘worst‐case scenarios’ is a common practice in the security domain, and since some ‘worst‐case scenarios’ could include civilizational collapse or human extinction, this should imply a strong aversion to risk. Although there are logical limits to the ‘precautionary principle’ with respect to existential risks,10 it has practical implications for security policy, such as taking preventive, cost‐effective, and long‐term oriented action (Clarke, 2005). More generally, making (existential) security a priority does not imply the sacrifice of all other values (e.g. political liberty, economic wealth), but it does mean that potential gains in other values be weighed against potential losses in security. Security is always a question of degree (Wolfers, 1952).

From what threats? Existential security is concerned with those threats that have their origins in human agency and could bring about civilizational collapse or human extinction. This requires broadening the security agenda beyond its conventional focus on ‘security from violence’, while excluding ‘natural’ existential risks (e.g. asteroids and supervolcanos). There are two main reasons for emphasizing anthropogenic threats. The first is the low probability of natural risks on timescales relevant to humanity (Bostrom, 2013; Bostrom and Cirkovic, 2008;), whereas anthropogenic threats are, by definition, relevant to human timescales, including the twenty‐first century (Rees, 2003). The second is that many prevention/mitigation strategies for anthropogenic existential threats act on their drivers in human agency, which makes little sense for natural risks. The spectrum of anthropogenic existential threats includes threats to international peace and security (e.g. nuclear war), dangers from human intervention in the natural environment (e.g. climate change), and risks from emerging technologies (e.g. AI). Existential security must take into account the complex relationships between human, environmental, and technological systems, as well as inherent uncertainties about existential threat scenarios (e.g. ‘nuclear winter’, ‘hothouse Earth’, or ‘superintelligence’).

By what means and modes of protection? The existential security frame requires innovation in the means and modes of security policy. This is because the conventional emphasis on military capabilities and balancing is either inadequate (e.g. nuclear war), irrelevant (e.g. climate change), or counterproductive (e.g. AI). Moreover, the pursuit of relative gains/losses in security is fundamentally misguided for anthropogenic existential threats, since – as a general principle – either all human societies are safe, or none of them are. Existential security requires a paradigm shift from thinking about security policy as a matter of (national) ‘defense’ to being a matter of (global) ‘governance’. Governance is not an end in itself (e.g. the creation of a ‘world state’), but rather a means to security (i.e. the survival of humankind). The pursuit of existential security requires means of protection that involve a comprehensive set of political, economic, and technological resources – not merely military capabilities. The modes of protection are primarily ‘restraint’ and ‘resilience’. Restraint is a prevention strategy, while resilience is a mitigation strategy, which take on different forms for different threats. For the nuclear threat, restraint manifests itself in the policies of disarmament, arms control, and nonproliferation, while resilience comes mostly in the form of nuclear bunkers and shelters (Bull, 1961; Deudney, 2007). For climate change, restraint is primarily about limiting greenhouse gas emissions and the degradation of carbon sinks, while resilience is about making societies less vulnerable to heat stress, rising seas, food and water scarcities, new diseases, and human migration (Wallace‐Wells, 2019; World Bank, 2012). For AI, restraint entails the slow and careful development of AI (Bostrom, 2014) – or perhaps forgoing the ‘AI dream’ altogether (Joy, 2000) – while resilience is about reducing societal vulnerability to technological disruption (e.g. cybersecurity). Importantly, the growing survival interdependence of human societies implies that restraint and resilience must be mutual to be effective. If only some states choose disarmament or nonproliferation, if some societies reduce carbon emissions while others increase them, or if one technology firm decides to rapidly pursue ‘superintelligence’, then the (in)action of some actors may affect the security of all humankind. This emphasis on mutual restraint and resilience contrasts with the national security frame's emphasis on ‘self‐help’.

### 2AC---No !---China Threat Construction

#### No self-fulfilling prophesy---theorizing about the danger of US-China war creates the caution and risk-aversion necessary to avoid it.

Wang 20, Professor of Political Science at Western Michigan University. He holds a Ph.D. in political science from the University of Chicago. (Yuan-kang, 11/9/20, "Roundtable 12-2 on *Thucydides’s Trap? Historical Interpretation, Logic of Inquiry, and the Future of Sino-American Relations*", *H-Diplo | ISSF*, https://issforum.org/roundtables/12-2-thucydides)

Throwing the Baby Out with the Bathwater?

Chan warns that the discourse on Thucydides’s Trap and power transition can create a self-fulfilling prophecy. If leaders believe in Thucydides’s Trap and act accordingly, it may create the anticipated conditions that make war more likely. Talking and thinking in terms of Thucydides’s Trap will influence the state’s construction of its identity as well as its definition of interests and preferences. The discourse is harmful because it encourages ‘othering’ the opponent and contributes to confrontation.

Should we, then, throw out the proposition that war is more likely when the system is undergoing a power transition?

It might be worthwhile to go back to what Thucydides’s Trap refers to: “the severe structural stress caused when a rising power threatens to upend a ruling one. In such conditions, not just extraordinary, unexpected events, but even ordinary flashpoints of foreign affairs, can trigger large-scale conflict.”[112] Instead of creating a self-fulfilling prophecy, this statement should induce caution from leaders in Beijing and Washington. Understanding the danger of war is the first step to avoid being trapped in it. Like Chan, Allison seeks to offer “a set of principles and strategic options for those seeking to escape Thucydides’s Trap and avoid World War III.”[113]

Obviously, historical analogies cannot completely capture an ongoing event. Allison himself cautions against “facile analogizing” and emphasizes that “the differences matter at least as much as the similarities.”[114] The purpose of analogizing Thucydides’s Trap is not to shoehorn China and the United States into the roles of Athens and Sparta respectively, as Chan suggests (17-18), but to underscore the enduring feature of international politics throughout the ages. The dynamics of conflict highlighted by Thucydides remain as relevant today as it was two thousand years ago.

Many scholars accuse structural theory of determinism, as Chan does, (14, 34), even though structuralists do not adopt it. States can go to war for a variety of reasons. Attempting to isolate a single cause for all wars is impossible. The proposition that war tends to break out during a power transition is better understood as a probabilistic—not deterministic—statement. The structural tensions cause by power shifts can substantially increase the probabilities of war, much like dry leaves waiting for a spark, but it does not mean that war will inevitably break out. Properly understood, Thucydides’s Trap cautions us to be prepared for the danger of war during a power transition.

Overall, Chan’s book provides a stronger critique of power transition theory than of Thucydides’s Trap. Students of power shifts should take his argument seriously and avoid the pitfalls he identifies. We should not, however, hastily dismiss the warnings of Thucydides’s Trap.

#### No impact to threat inflation:

#### 1---government officials are adept at accurately capturing China’s behavior. Empirics work, and purely academic accounts are inaccurate.

Chan 04, \*Steve Chan, College Professor of Distinction at the University of Colorado; (“Extended Deterrence in the Taiwan Strait: Learning from Rationalist Explanations in International Relations”, Asian Affairs: An American Review , Fall, 2004, Vol. 31, No. 3 (Fall, 2004), pp. 166-191)

Rationalist interpretations do not imply that people are omnipotent in their ability to procure and process information. We know all too well that people are subject to a variety of cognitive and perceptual errors (for example, Jervis 1976; Levy 1997; Kahneman and Tversky 2000; Tversky and Kahneman 1977). This recognition of limits to rationality, however, hardly warrants general attributions of naivete, even stupidity, to government leaders. On the contrary, it seems sensible to start from the premise that officials know their counterparts far better than scholars may wish to acknowledge. Washington, Beijing, and Taipei, for instance, invest enormous time, effort, and resources in trying to gain an accurate understanding of each other. Academics have a hard time claiming any special insight or unique source of wisdom, whether it is based on mastery of the other side's language, intimate familiarity with its culture, or access to timely and sensitive information with restricted distribution. If anything, they are usually at a considerable disadvantage on these scores when compared to diplomats, intelligence analysts, and even journalists and business people. Indeed, academics in fields such as history and political science typically operate in the realm of common knowledge, outdated information, and mundane data. This confession in turn implies that at least for some of us, our individual and collective forte lies with the analysis of persistent empirical patterns and the formulation of general models of foreign policy conduct.

#### 2---unfounded analysis is filtered out.

Ravenal 09, professor emeritus of the Georgetown University School of Foreign Service. He is an expert on NATO, defense strategy, and the defense budget. He is the author of Designing Defense for a New World Order (Earl, “What's Empire Got to Do with It? The Derivation of America's Foreign Policy,” *Critical Review: An Interdisciplinary Journal of Politics and Society*, 21.1)

Roles (all theorists state) give rise to “expectations” of performance. My point is that virtually every governmental role, and especially national-security roles, and particularly the roles of the uniformed military, embody expectations of devotion to the “national interest”; rationality in the derivation of policy at every functional level; and objectivity in the treatment of parameters, especially external parameters such as “threats” and the power and capabilities of other nations. Sub-rational models (such as “public choice”) fail to take into account even a partial dedication to the “national” interest (or even the possibility that the national interest may be honestly misconceived in more parochial terms). In contrast, an official’s role connects the individual to the (state-level) process, and moderates the (perhaps otherwise) self-seeking impulses of the individual. Role-derived behavior tends to be formalized and codified; relatively transparent and at least peer-reviewed, so as to be consistent with expectations; surviving the particular individual and transmitted to successors and ancillaries; measured against a standard and thus corrigible; defined in terms of the performed function and therefore derived from the state function; and uncorrrupt, because personal cheating and even egregious aggrandizement are conspicuously discouraged. My own direct observation suggests that defense decision-makers attempt to “frame” the structure of the problems that they try to solve on the basis of the most accurate intelligence. They make it their business to know where the threats come from. Thus, threats are not “socially constructed” (even though, of course, some values are). A major reason for the rationality, and the objectivity, of the process is that much security planning is done, not in vaguely undefined circum- stances that offer scope for idiosyncratic, subjective behavior, but rather in structured and reviewed organizational frameworks. Non-rationalities (which are bad for understanding and prediction) tend to get filtered out. People are fired for presenting skewed analysis and for making bad predictions. This is because something important is riding on the causal analysis and the contingent prediction. For these reasons, “public choice” does not have the “feel” of reality to many critics who have participated in the structure of defense decision-making. In that structure, obvious, and even not-so-obvious, “rent-seeking” would not only be shameful; it would present a severe risk of career termination. And, as mentioned, the defense bureaucracy is hardly a productive place for truly talented rent-seekers to operate, compared to opportunities for personal profit in the commercial world. A bureaucrat’s very self-placement in these reaches of government testifies either to a sincere commitment to the national interest or to a lack of sufficient imagination to exploit opportunities for personal profit.

### 2AC---China Threat

#### Don’t over-analyze China’s behavior---they mean what they say, and their intentions to upend the international system are opaque.

Brands 20, \*Hal Brands is an American scholar of U.S. foreign policy. He is the Henry A. Kissinger Distinguished Professor of Global Affairs at the Johns Hopkins University School of Advanced International Studies and a Resident Scholar at the American Enterprise Institute; (May 20th, 2020, “What Does China Really Want? To Dominate the World”, https://www.bloomberg.com/opinion/articles/2020-05-20/xi-jinping-makes-clear-that-china-s-goal-is-to-dominate-the-world)

Can we pay the Chinese Communist Party the compliment of acknowledging that it means what it says and knows what it wants? That may be the key to understanding Beijing’s strategic ambitions in the coming decades.

A long-standing trope in the U.S. [debate](https://warontherocks.com/2018/12/wotr-podcast-full-steam-ahead-naval-competition-with-china/) on [that](https://warontherocks.com/2019/01/the-party-congress-test-a-minimum-standard-for-analyzing-beijings-intentions/) [subject](https://www.brookings.edu/wp-content/uploads/2018/10/fp_20181018_us_china_transcript.pdf) is that China itself doesn’t know what it seeks to achieve, that its leaders haven’t yet worked out how far Beijing’s influence should reach. Yet there is a growing body of evidence, assembled and interpreted by talented China experts, that the Chinese government is indeed aiming for global power and perhaps global primacy over the next generation — that it seeks to upend the American-led international system and create at least a competing, quasi-world order of its own.

It doesn’t take unparalleled powers of deduction to reach this conclusion. Top Chinese officials and members of the country’s foreign policy community are becoming increasingly explicit in saying so themselves.

President Xi Jinping more than hinted at this goal in his landmark address to the 19th Party Congress in October 2017. That speech represents one of the most authoritative statements of the party’s policy and aims; it reflects Xi’s [understanding](https://twitter.com/PLMattis/status/1259592233726205953) of what China has accomplished under Communist rule and how it must advance in the future.

Xi [declared](http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf) that China “has stood up, grown rich, and is becoming strong,” and that it was now “blazing a new trail for other developing countries” and offering “Chinese wisdom and a Chinese approach to solving the problems facing mankind.” By 2049, Xi promised, China would “become a global leader in terms of composite national strength and international influence” and would build a “stable international order” in which China’s “national rejuvenation” could be fully achieved.

This was the statement of a leader who sees his country not just participating in global affairs but setting the terms, and it testifies to two core themes in China’s foreign policy discourse.

The first is a deeply skeptical view of the existing international system. Chinese leaders recognize that the global trade regime has been indispensable to the country’s economic and military rise. Yet when they look at the key features of the world Washington and its allies have made, they see mostly [threats](https://tnsr.org/2018/11/xis-vision-for-transforming-global-governance-a-strategic-challenge-for-washington-and-its-allies/).

In their view, American alliances do not preserve peace and stability; they stunt China’s potential and prevent Asian nations from giving Beijing its due. Seen through that lens, promoting democracy and human rights is neither moral nor benign, but propaganda supporting a dangerous doctrine that threatens to delegitimize the Communist government and energize its domestic enemies. U.S.-led international institutions appear as tools for imposing America’s will on weaker states. The Communist Party recognizes that the liberal international order has brought benefits, [writes](https://www.nbr.org/wp-content/uploads/pdfs/publications/sr83_chinasvision_jan2020.pdf) Nadege Rolland, a senior fellow at the National Bureau of Asian Research, but “the party abhors and dreads” the principles on which it is based.

The second theme is that the international order must change — not a little, but a lot — for China to become fully prosperous and secure. Chinese leaders have, understandably, been somewhat opaque in describing the world they want, but the outlines are becoming easier to discern.

If one studies the statements of Xi and other top officials, China expert Liza Tobin [concludes](https://tnsr.org/2018/11/xis-vision-for-transforming-global-governance-a-strategic-challenge-for-washington-and-its-allies/), what emerges is a vision in which “a global network of partnerships centered on China would replace the U.S. system of treaty alliances” and the world would view Chinese authoritarianism as preferable to Western democracy.

Based on a similar analysis, Rolland [agrees](https://www.nbr.org/wp-content/uploads/pdfs/publications/sr83_chinasvision_jan2020.pdf) that China has “a yearning for partial hegemony,” a loose dominance over large swaths of the global south. When it comes to global governance, still other [examinations](https://www.tabletmag.com/sections/news/articles/china-plans-global-order) [show](https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/), Beijing wants a system in which international institutions buttress rather than batter repressive regimes. Meanwhile, Chinese strategists and academics are talking openly about building a “new China-centric global economic order.”

There is little indication, in any of this, that Beijing’s strategic horizon is limited to the Western Pacific or even Asia. Xi’s [invocation](http://www.xinhuanet.com/english/2019-10/03/c_138445509.htm) of a “community with a shared future for humanity” [indicates](https://warontherocks.com/2019/01/the-party-congress-test-a-minimum-standard-for-analyzing-beijings-intentions/) a [global](https://tnsr.org/2018/11/xis-vision-for-transforming-global-governance-a-strategic-challenge-for-washington-and-its-allies/) tableau for Chinese influence. One hardly has to read between the lines to understand that this agenda will require fundamentally resetting the current geopolitical balance. As Xi remarked several years ago, China must work resolutely toward “a future where we will win the initiative and have the dominant position.”

Of course, there’s not need to take literally everything national leaders say, or even everything that makes it into official speeches. In Beijing’s case, however, Chinese leaders are actually saying less than what the country is doing.

Whether it is the naval shipbuilding program that is churning out vessels at astonishing rate; the drive to [control](https://www.bloomberg.com/opinion/articles/2020-03-31/china-s-influence-operation-goes-beyond-who-taiwan-and-covid-19) existing international organizations and build new ones; the projection of military power in the [Arctic](https://www.cambridge.org/core/books/china-as-a-polar-great-power/22493FFC041E6739DAED329CCB71F688#fndtn-information), the Indian Ocean and points beyond; the quest to [dominate](https://www.pbs.org/wgbh/frontline/article/made-in-china-2025-the-industrial-plan-that-china-doesnt-want-anyone-talking-about/) the world’s high-tech industries; the ever-more [systematic](https://halbrands.org/wp-content/uploads/2018/09/60-5-07-Brands.pdf) efforts to support authoritarian regimes and weaken democratic institutions; or the Belt and Road Initiative that [encompasses](https://tnsr.org/2019/07/unlocking-the-gates-of-eurasia-chinas-belt-and-road-initiative-and-its-implications-for-u-s-grand-strategy/) multiple continents, China is hardly acting like a country that lacks a grand geopolitical design.

As with so many aspects of the U.S.-China competition, there is a Cold War parallel. During the 1970s, some leading American Sovietologists insisted that Moscow was becoming a satisfied, status quo power. Yet that claim required ignoring what Soviet leaders [said](https://www.google.com/books/edition/What_Good_Is_Grand_Strategy/nGqoAgAAQBAJ?hl=en&gbpv=1&bsq=%22we%20make%20no%20secret%22) about detente and peaceful coexistence — that it was a way of ensuring the triumph of socialism without war — as well as their efforts to build military superiority and positions of strength in the Third World. The warning signs were evident then, as they are today.

China probably doesn’t have a step-by-step checklist for achieving global primacy, any more than the Soviet Union did in the 1970s. Chinese leaders aren’t insensitive to costs and obstacles: Xi may ritualistically restate the importance of unifying the Chinese nation, but that [doesn’t mean](https://twitter.com/resplinodell/status/1259883799254634498) he’s hell-bent on war over Taiwan.

Beijing may not even have decided which of its two paths to global influence is preferable: Establishing dominance in the Western Pacific and then expanding outward from there, or outflanking the U.S. position in the region by building up economic and political power around the world. Finally, China may ultimately fail to accomplish any of this. Perhaps the coronavirus will so weaken the U.S. and the liberal order that China’s ascent will be accelerated. Or perhaps China will run into so many internal problems, and so much external resistance, that its drive will stall.

Yet we ought to recognize that the debate about what China wants is growing stale, because China’s leaders and behavior have increasingly answered that question. When a proud and powerful challenger starts to advertise its global ambitions, Americans should probably err on the side of taking those ambitious seriously.

### 2AC---Deterrence Good

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

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

Counter-Pressure Works

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

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

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

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

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

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

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

### 2AC---AT: Alt---Desecuritization

#### Desecuritization is theoretically useless and does nothing.

Hynek 13, \*Nik Hynek, Prof of International Relations and Theory of Politics at the Metropolitan University Prague and Charles University, with David Chandler, (“No emancipatory alternative, no critical security studies”, Critical Studies on Security, 2013 Vol. 1, No. 1, 46–63, http://www.bristol.ac.uk/media-library/sites/spais/migrated/documents/cssrg1.pdf)

These ‘post-emancipatory’ scholars still frame Western and international intervention in potentially emancipatory terms, but the horizons and aspirations have been substantially lowered from the universalist call to radical academic policy advocacy, of the founders of emancipatory approaches within security studies. While the initial confident calls for emancipatory alternatives at least had an understanding of the need for emancipatory agency, unfortunately found only in Western powers and international institutions, the later approaches lack this clarity and confidence, merely suggesting that more ‘open’, ‘unscripted’, ‘locally sensitive’, ‘desecuritised’ and less ‘universalist’ and ‘liberal’ approaches can avoid the ‘resistances’ held to come from the local level. If these approaches are ‘emancipatory’ they lack any clear project or programme as to what these claims might mean or how they might be carried out in reality and are little different to mainstream think tank proposals calling for more ‘local ownership’, ‘local capacity-building’, ‘empowerment’, ‘sustainability’ and ‘resilience’ (see Chandler 2012, Forthcoming).