# Neg---AI Logistics---Starter Pack

## Cooperation Advantage

### 1NC---EU Turn

#### Plan prevents cooperation with EU---proliferates new agencies and makes coordination impossible

Simona R. Soare 21, was a Senior Associate Analyst at EUISS from 2019 to end May 2021. Her research focused on United States security policy, transatlantic security and EU-NATO relations. Prior to joining EUISS, Simona served as advisor to the Vice-President of the European Parliament (2015-2019) and as an analyst with the Romanian Ministry of Defence, working on transatlantic and European security. She has also been a research associate with the Institut d’Études Européennes (IEE) at Université Saint Louis-Bruxelles. Simona holds a PhD in Political Science from the National School for Political and Administrative Studies in Bucharest where she lectured on international security (2008-2015). She is the recipient of a U.S. Department of State fellowship on U.S. Grand Strategy and has published extensively on American and transatlantic security. "Innovation as Adaptation: NATO and Emerging Technologies" June 11. <https://www.gmfus.org/news/innovation-adaptation-nato-and-emerging-technologies> //pipk

Broadening and Regularizing NATO-EU Cooperation

The Biden administration also provides a window of opportunity to progress and be ambitious in broadening and regularizing NATO-EU cooperation in the field of innovation and EDTs. While political dialogue among their leadership has been steadily increasing over the past five years, the EU and NATO have consulted on their respective EDTs agendas only twice. Furthermore, bureaucratic procedures and misalignments sometimes frustrate even staff-to-staff cooperation in this area. The EU and increasingly NATO are proliferating agencies that conduct work on innovation in EDTs, including in security and defense. This makes it challenging to achieve internal coherence of activities within one organization, let alone coordinating agendas between the two.

As the allies meet with the EU High Representative for Foreign Affairs and Security Policy Josep Borrell at this month’s NATO summit, the two organizations need a more ambition agenda for cooperation. In particular, the EU and NATO need to consider a joint task force on fostering defense innovation and EDTs, with renewable two-year mandates. This instrument would provide political impetus for closer cooperation on EDTs, it would give coherence, regularity, and structure to the efforts of the two sides, and ensure commonality of purpose and synergy of output. In addition, allies could consider meeting regularly in EU-NATO digital summit formats. The EU could take the lead in this regard given its considerable financial capacity for investing in EDTs and its regulatory powers. EU-NATO digital summits would allow the transatlantic partners to regularly review progress, provide strategic guidance on legal, ethical and adoption challenges related to innovation and EDTs, and enhance their tech diplomacy by inviting like-minded global partners to attend.

### 1NC---Governance Bad

#### Regulation destroys AI control by driving it underground, abroad, or into higher-risk areas

Dr. Nell Watson 21, PhD in Engineering from the University of Gloucestershire, Degree in AGI Safety Fundamentals from the University of Cambridge, Senior Scientific Advisor to The Future Society at Harvard University, Fellow at the British Computing Society and Royal Statistical Society, “Regulatory Challenges to Catastrophic AI Risk”, ExO Insight, 11/24/2021, https://insight.openexo.com/regulatory-challenges-to-ai/

Rick Increase Factors:

Obfuscation: Regulations may drive research underground where it is harder to monitor, or to ‘flag of convenience’ jurisdictions with lax restrictions, by embedding dangerous technologies within apparently benign cover operations (multipurpose technologies), or by obfuscating the externalized effects of a system, such as in the vehicle emissions scandal (Wikipedia).

Arms race: Recent advances in machine learning such as multimodal abstractions models (aka Transformers, Large Language Models, Foundation Models) such as GPT-3 and DALL-E illustrate that dumping computing resources (and the funds for them) in colossal models seems to be a worthy investment. So far, there is no apparent limit or diminishing return on model size, and so now state and non-state actors are scrambling to produce the largest models feasible in order to access thousands of new capabilities never before possible. An arms race is afoot. Such arms races can lead to rapid and unexpected take-off in terms of AI capability, and the rush can blindside people to risks, especially when the loss of a race can mean an existential threat to a nation or organization.

Perverse incentives: Incentives can be powerful forces within organizations, and financialization, moral panic, or fear of political danger may cause irrational or incorrigible behavior of personnel within organizations.

Postmodern Warfare: Inexpensive Drones and other AI-enabled technologies have tremendous disruptive promise within the realm of warfare, especially given their asynchronous nature. Control of drone swarms must be performed using AI technologies, and this may encourage the entire theatre of war to be increasingly delegating to AI, perhaps including the interpretation of rules of engagement and grand strategy. (Lsusr, 2021)

Cyber Warfare: Hacking of systems is increasingly being augmented with machine intelligence (Cisomag, 2021), through GAN-enabled password crackers (Griffin, 2019) and advanced social engineering tools (Newman, 2021). This is equally the case in the realm of defense, where only machine intelligence may provide the swift execution required to defend systems from attack. A lack of international cyberwar regulations, and poor international policing of organized cybercrimes, may increase the risk of catastrophic risks to societal systems.

Zersetzung: The human mind is becoming a new theatre of war, through personalized generative propaganda, which may even extend to gaslighting attacks on targeted individuals, significantly leading to destabilization of societies (Williams, 2021). Such technologies are also plausibly deniable, being difficult to prove who may be responsible.

Inflexibility: The German Military after WW1 was not allowed to develop their artillery materiel, and so developed powerful rocket technologies instead, as these were not subject to regulation. Similarly, inflexible rules may permit exploitable loopholes. They may also not be sufficiently adaptive to allow for the implementation of new technologies and even improved industry standards.

Limitation of problem spaces: – It may be taboo to allow machine intelligence to work on sensitive issues or to be exposed to controversial (if potentially accurate) datasets. This may limit the ability of AI to make sense of out complex issues, and thereby frustrate finding solutions for crises.

#### That causes catastrophic AI since it’ll be controlled by rogues with no precautions AND without defensive countermeasures

Robert A. Freitas 22 Jr., JD from the University of Santa Clara (Santa Clara, CA), School of Law, Research Fellow at the Institute for Molecular Manufacturing, Won the 2009 Feynman Prize in Nanotechnology for Theory, BS in Physics and Psychology from Harvey Mudd College, “Molecular Manufacturing: Too Dangerous to Allow?”, Nanotechnology Perceptions, Volume 2, Number 1, Republished at The Lifeboat Foundation, https://lifeboat.com/ex/molecular.manufacturing

Attempts to block or “relinquish” [3, 12] molecular manufacturing research will make the world a more, not less, dangerous place [13]. This paradoxical conclusion is founded on two premises. First, attempts to block the research will fail. Second, such attempts will preferentially block or slow the development of defensive measures by responsible groups. One of the clear conclusions reached by Freitas [4] was that effective countermeasures against self-replicating systems should be feasible, but will require significant effort to develop and deploy. (Nanotechnology critic Bill Joy, responding to this author, complained in late 2000 that any nanoshield defense to protect against global ecophagy “appears to be so outlandishly dangerous that I can’t imagine we would attempt to deploy it.” [12]) But blocking the development of defensive systems would simply insure that offensive systems, once deployed, would achieve their intended objective in the absence of effective countermeasures. James Hughes [13] concurs: “The only safe and feasible approach to the dangers of emerging technology is to build the social and scientific infrastructure to monitor, regulate and respond to their threats.”

We can reasonably conclude that blocking the development of defensive systems would be an extraordinarily bad idea. Actively encouraging rapid development of defensive systems by responsible groups while simultaneously slowing or hindering development and deployment by less responsible groups (“nations of concern”) would seem to be a more attractive strategy, and is supported by the Foresight Guidelines [10]. As even nanotechnology critic Bill Joy [14] finally admitted in late 2003: “These technologies won’t stop themselves, so we need to do whatever we can to give the good guys a head start.”

While a 100% effective ban against development might theoretically be effective at avoiding the potential adverse consequences, blocking all groups for all time does not appear to be a feasible goal. The attempt would strip us of defenses against attack, increasing rather than decreasing the risks. In addition, blocking development would insure that the substantial economic, environmental, and medical benefits [15] of this new technology would not be available.

Observes Glenn Reynolds [16]:

To the extent that such efforts [to ban all development] succeed, the cure may be worse than the disease. In 1875, Great Britain, then the world’s sole superpower, was sufficiently concerned about the dangers of the new technology of high explosives that it passed an act barring all private experimentation in explosives and rocketry. The result was that German missiles bombarded London rather than the other way around. Similarly, efforts to control nanotechnology, biotechnology or artificial intelligence are more likely to drive research underground (often under covert government sponsorship, regardless of international agreement) than they are to prevent research entirely. The research would be conducted by unaccountable scientists, often in rogue regimes, and often under inadequate safety precautions. Meanwhile, legitimate research that might cure disease or solve important environmental problems would suffer.

#### AI regulation overshoots, destroying productive applications necessary to prevent existential catastrophes

Gönenç Gürkaynak 18, Founding Partner of ELIG Gürkaynak Attorneys-at-Law, LL.M. from Harvard Law School, İlay Yılmaz, Partner at ELIG Gürkaynak Attorneys-at-Law, and Güneş Haksever, LLM from Istanbul Bilgi University, Attorney at IBM Turkey, “Stifling Artificial Intelligence: Human Perils”, Computer Law & Security Review, Volume 32, Issue 5, 12/12/2018, https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3285264

Although scientists have calculated the significant positive welfare effects of Artificial Intelligence (AI), fear mongering continues to hinder AI development. If regulations in this sector stifle our active imagination, we risk wasting the true potential of AIs dynamic efficiencies. Not only would Schumpeter dislike us for spoiling creative destruction, but the AI thinkers of the future would also rightfully see our efforts as the ‘dark age’ of human advancement. This article provides a brief philosophical introduction to artificial intelligence; categorizes artificial intelligence to shed light on what we have and know now and what we might expect from the prospective developments; reflects thoughts of worldwide famous thinkers to broaden our horizons; provides information on the attempts to regulate artificial intelligence from a legal perspective; and discusses how the legal approach needs to be to ensure the balance between artificial intelligence development and human control over them, and to ensure friendly artificial intelligence.

Our technology, our machines, is part of our humanity. We created them to extend ourselves, and that is what is unique about human beings. – Ray Kurzweil1

1. Introduction

The Chinese cardboard game “Go” is one of the most complex strategy games humankind invented. Go was considered so important, there are myths indicating that ancient kings played Go between their armies in the battlefield to resolve the conflict in peace. Computers prevailed against humanities best in many zero-sum, perfect-information, partisan, deterministic strategy games2 before, with the exception of Go, which was something to be proud of.

The strategy aspect of Go is very complex and emphasizes the importance of balance on multiple levels and has internal tensions. A game of Go cannot be won by using brute force: calculating every possible move, similar to what IBM®’s then state of the art AI, Deep Blue® used to win over Gary Kasparov. To manoeuvre through the countless possible moves on the Go board and chose the most efficient path, one requires capabilities beyond the conventional computing powers; capabilities only our minds have (or so we thought), such as extremely accurate image and pattern recognition and insight, all of which we thought granted us superiority over the artificial minds we created.

In October 2015, a software called “AlphaGo®” became the first computer to beat a professional human Go player in an un-handicapped game of Go (Silver and Hassabis, 2016). AlphaGo’s victory is probably one of the most significant demonstrations of the capabilities of an AI. Firstly, it shows that AIs are beginning to surpass us at things where success is dependent on strategy as well as calculation. Things we classify as a “game”, from stock exchange to conflicts, from contract negotiations to hostage situations. Second, AlphaGo developed strategies on its own, through playing millions of games against itself. These feats sent the chills down the spines of those who fear that AIs will overpower us in the future.

We humans accelerate the future with our minds. This is a strength and a weakness. Often, our predictions of the future are highly inaccurate. Based on predictions from a book called ‘The World in 2010’, published in 1976, we should have been living above and below the surfaces of three planets as of five years ago. Predictions regarding the future of AI are equally likely to be off base.

To avoid premature regulation over AI, we should be studying and searching for the meaningful point in time when a broader anxiety about AI becomes a genuine concern. The study of a point of ripeness, a ‘threshold ability test,’ asks when AI could really bring about concrete disadvantages that might counter-balance the demonstrated contribution to economic efficiency and welfare.

In the absence of such an objective benchmark marking the point in time when AI becomes a competitor with the human mind, regulators could easily jump the gun in regulating AI, which would lead to irreparable harm in total welfare of human societies.

Most of what we consider AI today is really our own intelligence re-formatted and re-cycled, with the help of computers lacking any skill of learning or consciousness of being. Regulation at this stage would be perverse. The economic efficiency potentials of AI should be set entirely free at this point in time, allowing us to actively and aggressively research appropriate goals for them which would not result in the extinction of humankind.

If you think our future robot overlords will one day thank us for ignoring the risks and under regulating, think again. On the one hand, any issues we may face from AIs will likely result from humanity failure to effectively direct AIs to our needs, not because we switched to a defensive AI regulation regime too early. On the other hand, at some point of time in the not too distant future, natural, human-related or external factors may threaten the fate of the Earth, and we may need AI to save the planet and us. One hopes that society has not pulled the hand brakes on the wheels of AI too early, fearing our own active imagination.

#### AI controls are inevitable, but will be gradual and incrementally ratchet up over time---they’ll start with liability and transparency, then move into specific applications, solving downside risk without imposing premature and ineffective regulation

Chris Reed 18, Professor of Electronic Commerce Law at Queen Mary, University of London, LLM from the University of London, “How Should We Regulate Artificial Intelligence?”, Philosophical Transactions of the Royal Society B, Volume 376, Issue 2128, 9/13/2018, https://royalsocietypublishing.org/doi/10.1098/rsta.2017.0360

Using artificial intelligence (AI) technology to replace human decision-making will inevitably create new risks whose consequences are unforeseeable. This naturally leads to calls for regulation, but I argue that it is too early to attempt a general system of AI regulation. Instead, we should work incrementally within the existing legal and regulatory schemes which allocate responsibility, and therefore liability, to persons. Where AI clearly creates risks which current law and regulation cannot deal with adequately, then new regulation will be needed. But in most cases, the current system can work effectively if the producers of AI technology can provide sufficient transparency in explaining how AI decisions are made. Transparency ex post can often be achieved through retrospective analysis of the technology's operations, and will be sufficient if the main goal is to compensate victims of incorrect decisions. Ex ante transparency is more challenging, and can limit the use of some AI technologies such as neural networks. It should only be demanded by regulation where the AI presents risks to fundamental rights, or where society needs reassuring that the technology can safely be used. Masterly inactivity in regulation is likely to achieve a better long-term solution than a rush to regulate in ignorance.

This article is part of a discussion meeting issue ‘The growing ubiquity of algorithms in society: implications, impacts and innovations'.

1. Introduction

It is hardly surprising that there has been a sudden interest in regulating artificial intelligence (AI). AI technology has moved from the research laboratory to become part of our daily lives with remarkable speed. We have seen the first fatal accident involving an autonomous vehicle [1,2], AI applications are analysing images to detect potentially cancerous cells [3] and numerous other implementations are in place or in the pipeline.

The introduction of AI technologies creates societal risks. Although AI technologies aim to augment or replace human decision-making, leading to fewer wrong decisions, there is no doubt that AI will still get it wrong sometimes. And the ways in which AI gets it wrong are likely to be very different from the ways in which a human would make mistakes. This feels dangerous to society. We want to know the kinds of risks we are running, and purely statistical arguments that AI makes us safer are not convincing to the wider population.

Good regulation would improve our perception of safety, and also our perception that humans remain in control. It could also mitigate any new risks which the use of AI creates. But bad regulation risks stifling the development and implementation of useful AI solutions, perhaps even without improving safety and control. Thus, we need to understand what regulation can and cannot do so that we can shape it appropriately. It is also important that those who produce and use AI technologies are actually able to comply with regulation, and that regulation does not stifle worthwhile advances in the technology. Outside specifically regulated sectors, the general approach of law and regulation is that innovation is freely permitted, but that those responsible must bear the consequences if that innovation causes certain types of harm. If our existing law and regulation can deal with AI innovation in that way, no immediate change is needed. The argument, if one exists, for requiring all those who adopt an AI technology to demonstrate that it achieves a higher standard of performance and reliability than other innovations has not yet been made out.

2. The problem

Fundamentally, the problem which regulation must seek to solve is that of controlling undesirable risks. For any truly useful AI technology, there is likely to be empirical evidence that it is more cost-effective and, ideally, more accurate at making decisions than the human-based solution it replaces. But that evidence will be based on comparison with the human-based solution, whose deficiencies are currently tolerated by society. An AI-based solution will have its own deficiencies, and these will be less acceptable if they produce wrong answers where a human would have decided correctly. Regulation ought therefore to focus on any new risks which the AI solution presents, recognizing that some of these risks will be as yet unknown.

Some commentators are so alarmed by the prospect of unknown risks that they have proposed the establishment of a general regulator for AI [4]. But, there are three strong arguments against introducing new, generally applicable legal and regulatory obligations at this moment.

First, any regulatory body needs a defined field of operation, and a set of overriding principles on the basis of which it will devise and apply regulation. Those principles will be based on mitigating the risks to society which the regulated activity creates. Until the risks of AI are known, at least to some degree, this is not achievable. Regulation cannot control unknown risks, and devising a regulatory mandate on the basis of speculative risks seems unlikely to produce successful results.

Second, lawmakers are generally unsuccessful at prospective regulation, particularly in technology fields. The history of legislating prospectively for the digital technologies is one of almost complete failure [5].

Finally, and most importantly, a regulatory regime which aimed to deal with all uses of AI technology would be impossibly wide in scope. The range of potential applications is far too diverse, and it would be foolish to apply the same regulatory regime to autonomous vehicles as to smart refrigerators which order groceries based on consumption patterns. Probably, there is no plausible, let alone compelling, reason to regulate smart refrigerators at all. A regulatory project of this kind would risk becoming a project to regulate all aspects of human life.

The better strategy is to approach the problem incrementally. Some of the risks likely to be posed by AI technology are already apparent, and legal or regulatory action can be taken now to deal with them. Others will make themselves known as the technology becomes more widely used and can be dealt with in the same way. At some point, it will become apparent whether specific regulation is needed, and if so the scope and focus of that regulation will be possible to devise. But at present, we are some distance away from that point.

### 2NC---Offshoring

#### Offshoring’s quick, easy, and guaranteed by overwhelming economic incentives---it zeros solvency

Matthew U. Scherer 16, Senior Policy Counsel for Worker Privacy at the Center for Democracy & Technology, J.D. from Georgetown University Law Center, Former Editor-in-Chief of The Georgetown Journal of Legal Ethics, M.S. in Educational Policy from the University of Pennsylvania’s Graduate School of Education, Attorney at Buchanan Angeli Altschul & Sullivan LLP, “Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies”, Harvard Journal of Law and Technology, 29 Harv. J. Law & Tec 353, Volume 29, Number 2, Spring 2016, Lexis

The sources of public risk that characterized the twentieth century -- such as nuclear technology, mass-produced consumer goods, industrial-scale pollution, and the production of large quantities of toxic substances -- required substantial infrastructure investments. This simplified the regulatory process. The high cost of building the necessary facilities, purchasing the necessary equipment, and hiring the necessary labor meant that large corporations were the only non-governmental entities capable of generating most sources of public risk. Moreover, the individuals responsible for installing, operating, and maintaining the infrastructure typically had to be at the physical site where the infrastructure was located. The physical visibility of the infrastructure -- and of the people needed to operate it -- made it extremely unlikely that public risks could be generated clandestinely. 61 Regulators thus had little difficulty determining the "who" and "where" of potential sources of public risk.

By contrast, AI research and development can be performed relatively discreetly, a feature that AI shares with many other Information Age technologies. In 2009, Professor John McGinnis wrote that "[a]rtificial intelligence research is done by institutions no richer than colleges and perhaps would require even less substantial resources." 62 This actually overstated the resources necessary to participate in AI development, particularly with the rise of open-source programming. Simply put, a person does not need the resources and facilities of a large corporation to write computer code. Anyone with a reasonably modern personal computer (or even a smartphone) and an Internet connection can now contribute to AI-related projects. Individuals thus can participate in AI development from a garage, a dorm room, or the lobby of a train station. This potential for discreetness provides the most jarring difference between AI and earlier sources of public risk.

The participants in an AI-related venture may also be remarkably diffuse by public risk standards. Participants in an AI-related project need not be part of the same organization -- or, indeed, any organization at all. Already, there are a number of open-source machine-learning libraries; widely dispersed individuals can make dozens of modifications to such libraries on a daily basis. 63 Those modifications may even be made anonymously, in the sense that the identity in the physical world of individuals making the modifications is not readily discernible. 64

The AI program itself may have software components taken from multiple such libraries, each of which is built and developed discretely from the others. 65 An individual who participates in the building of an open-source library often has no way of knowing beforehand what other individuals or entities might use the library in the future. Components taken from such libraries can then be incorporated into the programming of an AI system that is being developed by an entity that did not participate in assembling the underlying machine-learning library.

These characteristics are not limited to open-source projects or freely available material. Many modern computer systems use commercial off-the-shelf ("COTS") hardware and software components, most of which are proprietary. 66 The ease with which such components can be acquired makes it tempting to maximize use of COTS components to control costs, despite the potential security issues associated with using software components developed wholly outside the system developer's control. 67 Modern AI programming is no exception; few, if any, AI systems are built from the ground up, using components and code that are wholly the creation of the AI developers themselves. Moreover, if past is prologue, the physical components of an AI system will be manufactured by yet other entities separate from those that developed the AI system's programming. While separately developed components are present in all complex machinery to a certain extent, the level of discreteness and the scale of interactivity between software and hardware components in modern computer systems already rivals or exceeds that of prior technologies, and that complexity seems likely to increase further with the development of stronger forms of AI. 68

In all likelihood, there will be considerable variation in the discreteness of the components of AI projects. Some AI systems likely will be built primarily with COTS or freely available hardware and software components, while others will mostly utilize programming and physical components designed and developed specifically for the AI project in question. Because of the cost advantages inherent in maximizing the use of COTS and freely available components, however, it seems all but certain that some AI systems will operate using a mishmash of hardware and software components harvested from many different companies. The interaction between numerous components and the disparate geographic locations of the companies involved will greatly complicate any regime designed to manage the risks associated with AI. 69

Finally, the inner workings of and the interactions between the components of an AI system may be far more opaque than with earlier technologies. COTS software components may be easy to acquire, but their coding often is proprietary. Critical features underlying an AI system's operation thus may not be immediately apparent or readily susceptible to reverse engineering. Contrast this with automobiles -- one of the twentieth century's great sources of public risk. Automobiles consist of approximately 30,000 individual physical parts, 70 but the ways in which those physical components interact is well understood -- not only by the designers and manufacturers of the vehicle itself, but also by the makers of parts for the vehicle and mechanics responsible for repairing the vehicles after they reach consumers. It seems unlikely that AI systems will demonstrate similar transparency if their development follows now-prevailing trends in information technology. Defects in the design of a complex AI system might be undetectable not only to consumers, but also to downstream manufacturers and distributors. 71

Taken together, these characteristics confront regulators with fundamental logistical difficulties that were not present in earlier sources of public risk. Participants in AI projects may be located in multiple countries and have no legal or formal contractual relationship with one another. Attempts by any one country to regulate their citizens' participation in such projects may not greatly impact the projects' development. Even for projects involving large firms, the relatively low cost of infrastructure and the small physical footprint required for AI development means that firms could simply move AI development work offshore if regulations in their country of origin prove too intrusive. Many would likely do so given the competitive advantages that accompany advances in AI. 72 [FOOTNOTE] 72 See, e.g., Vernor Vinge, The Coming Technological Singularity: How to Survive in the Post-Human Era, 10129 NASA CONF. PUBLICATION 11, 15 (1992), http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19940022855.pdf [https://perma.cc/J2SU-UK5E] ("In fact, the competitive advantage . . . of every advance in automation is so compelling that passing laws, or having customs, that forbid [human-level AI] merely assures that someone else will get them first."). [END FOOTNOTE]

#### They’ll move to havens with lax standards to dodge regulation

Dr. Amanda Askell 19, Research Scientist on the Policy Team at OpenAI, PhD in Philosophy from New York University, Dr. Miles Brundage, AI Policy Research Fellow with the Centre for the Governance of AI at Future of Humanity Institute, PhD in Human and Social Dimensions of Science and Technology from Arizona State University, and Gillian Hadfield, Schwartz Reisman Chair in Technology and Society, Professor of Law, and Professor of Strategic Management at the University of Toronto, PhD in Economics from Stanford University, “The Role of Cooperation in Responsible AI Development”, Computers and Society, https://arxiv.org/abs/1907.04534

1.4.4 The difficulty of constructing effective AI regulation

There is currently little in the way of AI-targeted regulation, including government regulation, industry self-regulation, international standards, and clarity on how existing laws will be applied to AI (see note 13). Well-designed regulatory mechanisms can incentivize companies to invest appropriate resources in safety, security, and impact evaluation when market failures or coordination failures have weakened the other incentives to do so. Poorly-designed regulation can be harmful rather than helpful, however. Such regulation can discourage innovation (Heyes, 2009) and even increase risks to the public (Latin, 1988).

AI regulation seems particularly tricky to get right, as it would require a detailed understanding of the technology on the part of regulators.21 The fact that private AI companies can generally relocate easily also means that any attempt to regulate AI nationally could result in international regulatory competition rather than an increase in responsible development.22 Regulation that is reactive and slow may also be insufficient to deal with the challenges raised by AI systems. AI systems can operate much faster than humans, which can lead to what Johnson et al. (2013) call ‘ultrafast extreme events’ (UEEs) such as flash crashes caused by algorithmic trading.23

### 2NC---Offshoring Impact---Turns Bad AI

#### Offshoring worsens AI danger---it’ll be constrained by U.S. social norms, but not if it moves abroad

John O. McGinnis 17, George C. Dix Professor in Constitutional Law at Northwestern University and a Contributing Editor at Law & Liberty, Graduate of Harvard College, Balliol College, Oxford, and Harvard Law School, “Accelerate Rather than Regulate Artificial Intelligence”, Law & Liberty, 7/19/2017, <https://lawliberty.org/accelerate-rather-than-regulate-artificial-intelligence/> [language modified]

But trying to slow down or have the government direct and restrict AI (which is much the same thing) in the United States would only allow other nations to advance AI faster. And since AI is at the heart of modern military operations, the United States would lose its essential military advantage. If the United States remains the best hope for freedom for [hu]mankind, certainly as compared to China, our greatest competitor in AI, that is a disastrous geopolitical policy.

Indeed, even without regulation my great fear is that the United States will fall behind China in developing AI. Given that data is what trains modern AI, China’s sheer size gives it an advantage because it generates more data. And even beyond its potentially larger pool of researchers, its universities are more geared to the sciences than are ours. Of course the United States does have advantages, such as finer top universities and a more attractive, more free society. Thus, what the United States can best do to accelerate AI here is to give after an appropriate security vetting a green card to any Ph.D from a bona fide university or to any student who has been accepted here to a doctorate program in computer science. And as I have suggested, it should also accelerate government grants to encourage the development of a friendly AI–one that is not dangerous to humans.

These policies would not only help maintain the security of the United States, but would give us the best chance of forestalling malevolent AI. That kind of AI is more likely to be developed in less free societies, because the social norms of those society will subject researchers to less criticism for such development. Moreover, accelerating the development of friendlier AI would create better machine intelligence to help forestall the less friendly kind.

Ever stronger AI is on the horizon. The only question is where it will be developed most quickly. The world will be better off if that place is the United States.

### 2NC---Countermeasures---Offshoring

#### Even the strictest possible regs won’t stop determined scientists and even one is enough---the only check is quickly deployable defensive tech BUT that’s wrecked by regulation

Ray Kurzweil 18, Received 21 Honorary Doctorates, Received the 1999 National Medal of Technology and Innovation, American Inventor and Futurist, Member of the National Academy of Engineering, BS in Computer Science from MIT, “The Deeply Intertwined Promise and Peril of GNR”, Artificial Intelligence Safety and Security, Ed. Yampolskiy, p. 31

Insights from the brain-reverse-engineering effort, overall research in developing AI algorithms, and ongoing exponential gains in computing platforms make strong AI (AI at human levels and beyond) inevitable. Once AI achieves human levels, it will necessarily soar past it because it will combine the strengths of human intelligence with the speed, memory capacity, and knowledge sharing that nonbiological intelligence already exhibits. Unlike biological intelligence, nonbiological intelligence will also benefit from ongoing exponential gains in scale, capacity, and price-performance.

Totalitarian relinquishment. The only conceivable way that the accelerating pace of advancement on all of these fronts could be stopped would be through a worldwide totalitarian system that relinquishes the very idea of progress. Even this specter would be likely to fail in averting the dangers of GNR because the resulting underground activity would tend to favor the more destructive applications. This is because the responsible practitioners that we rely on to quickly develop defensive technologies would not have easy access to the needed tools. Fortunately, such a totalitarian outcome is unlikely because the increasing decentralization of knowledge is inherently a democratizing force.

### 2NC---Superweapons---Offshoring

#### They’ll move to DEWs, heliobeams, or gravity weapons---those destroy the universe!

Phil Torres 18, Affiliate Scholar at the Institute for Ethics and Emerging Technologies, Founder of the X-Risks Institute, Writer Appearing in Skeptic, Free Inquiry, Bulletin of the Atomic Scientists, Salon, Truthout, Erkenntnis, Metaphilosophy, Foresight, Journal of Future Studies, and the Journal of Evolution and Technology, “Should Humanity Colonize Space?”, Medium, 3/31/2018, https://medium.com/@philosophytorres/should-humanity-colonize-space-181ca78905fd

Second, there could be so many different species and civilizations in the future that determining who exactly perpetrated an attack could pose an impossibly complicated forensic challenge. This too could undercut the threat of retaliation.

And third, so could the weapons available to technologically advanced future civilizations. For example, the US military is already experimenting with “direct-energy weapons” (DEWs) like laser and particle-beam weapons that can attack a target at or nearly at the speed of light. Since nothing travels faster than light — not even a message saying, “Help us, we were just attacked!” — the use of powerful DEWs by a Kardashev type II civilization, for example, could eliminate the threat of a counterstrike.

This differs from the Cold War situation in which each side could detect nuclear missiles traveling through the air with enough time to consult the relevant decision-making bodies and determine whether or not to strike back. Civilizations couldn’t possibly see a deadly laser beam that destroys crucial infrastructure coming; the damage would occur before a warning message from allies could ever reach them.

There are also biological and nanotech agents that civilizations could launch across the galaxy at each other, martial von Newman probes that are aided by metamaterial invisibility cloaks, “heliobeams” that concentrate large amounts of solar radiation on targets, and maybe even “gravity weapons” that use gravitational waves to create black holes (a speculative idea that appears to fall within the realm of physical possibility). Even more, the universe is teaming with asteroids and comets that could be catapulted toward planets or spaceships, with more destructive consequences than a swarm of hydrogen bombs. Some have called these “planetoid bombs,” since asteroids and comets are “planetoids.”

We also shouldn’t overlook the possibility that future civilizations devise entirely novel “weapons of total destruction” (WTDs). Just as our Paleolithic ancestors would be dumbstruck by the extraordinary mechanisms of mass death available to modern humans, so too might we be horrified by the weapons that our spacefaring children invent — say, WTDs that move at close to lightspeed and wreak galactic- or cosmic-scale hazards.

The cherry on the cake is that even a perfectly peaceable civilization might have strong incentives to obliterate its neighbors. For example, imagine two civilizations with radically different political, cultural, and religious traditions. They can’t even communicate very well because they speak entirely different languages and have evolved, through natural selection and cyborgization, divergent emotional repertoires and mental categories. They have different internal models of the world, distinct perceptual and phenomenological experiences, and incompatible “normative” worldviews.

Consequently, neither is able to trust the other. The result is that it would be rational for each to annihilate the other merely to ensure that the other doesn’t annihilate one first. Worse, if a civilization X believes that a civilization Y is rational, then X will believe that Y believes that it should annihilate X so that X doesn’t annihilate Y, since X annihilating Y would be the rational thing to do. (Whew!) This line of reasoning provides X an even stronger reason to annihilate Y, and therefore Y an even stronger reason to annihilate X — thus yielding a “spiral” of escalating tensions that ultimately culminates in war, despite both X and Y wishing for peace. Scholars know this as the “Hobbesian trap.”

But civilizations may have an equally strong incentive to destroy their neighbors even if they believe that those neighbors are irrational (rather than rational). For example, consider a civilization A that is full of irresponsible particle physicists. Civilization A has no bad intentions, yet it conducts physics experiments that could inadvertently end the universe. Another civilization B might try to reason with A not to conduct these experiments, but let’s imagine that A ultimately resists. In order to save A from annihilating the universe by accident, B may thus opt to launch a preemptive attack against A to avert a cosmic disaster.

Generalizing this case, since any given civilization will have some probability of accidentally destroying the universe, it would be in every civilization’s self-interest to destroy everyone else merely to obviate accidental cosmic calamities. This may be especially true if evolutionary adaptive radiation produces numerous species unable to fully grasp each others’ intentions, cognitive abilities, or moral values. The possibilities for miscommunication here are immense — and this should worry rather than reassure us.

### 2NC---Good AI---Link

#### It’s impossible to only regulate ‘bad’ AI without stifling the ‘good’. Tech is too far off and unpredictable AND humans have no current baseline for understanding, let alone assessing or guiding, productive means. Premature regulation drives straight to extinction.

Gönenç Gürkaynak 18, Founding Partner of ELIG Gürkaynak Attorneys-at-Law, LL.M. from Harvard Law School, İlay Yılmaz, Partner at ELIG Gürkaynak Attorneys-at-Law, and Güneş Haksever, LLM from Istanbul Bilgi University, Attorney at IBM Turkey, “Stifling Artificial Intelligence: Human Perils”, Computer Law & Security Review, Volume 32, Issue 5, 12/12/2018, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285264> [note – ‘ANI’ = ‘artificial narrow intelligence’]

3. Protecting human dominance through regulation or setting tailored goals to maintain human existence

Having a timeless and robust definition of AI is of paramount importance when thinking of regulating AI. One cannot regulate a certain subject without establishing a robust definition of what it regulates. The ambiguity of the definition of AI is mainly due to the “I”, “intelligence” of the AI. Concepts like “intelligence”, “consciousness”, “free will” and “soul” accompanying it are yet to have deterministic definitions although the greatest minds of our planet have tackled them for thousands of years (Burkeman, 2015).21

Neither any of the foregoing definitions of AI, nor many other definitions in the academia presents adequate definitions that can be satisfactory when regulation techniques are considered. In addition, the lack of definition is only one of the problems regulators will face; they will need to tackle liability gaps, control and transparency problems (Danaher, 2015).

In light of the foregoing, our primary statement stands firm: it is very early to begin thinking about regulating AIs or AI studies, particularly if such regulations may hinder developments that could prove essential for human existence. The turning point in AI development will probably be the development of ANIs, which should be encouraged through regulation, not restricted. However, if humanity fails in establishing adequate safe guards for ANIs, science fiction may turn into reality. Goertzel and Pitt (2012) call this the ‘AGI Sputnik moment’.

3.1. The great AI hype of 2015

Elon Musk’s and Stephen Hawking’s fears, Bill Gates’ cautious approach, Kurzweil’s optimistic take and Bostrom’s realistic analysis on the future that will probably be painted by AIs point to a single fundamental and existential dilemma: Are we going to be extinct because of AIs or will we maintain our existence with the help of AIs?

The cycle of extinction and rise of species may be the greatest success of evolution: ensuring the continuity of life. Over 90% of all species that ever existed on Earth went extinct and humanity’s fate will be no different, unless we come up with methods to achieve transcendence over evolution.22 Urban (2015) also treats this concept with a less theatrical manner and stresses two major outcomes for a possible ‘ASI Sputnik moment’. He states that either the introduction of ASIs will make immortality possible for our species or it will drive the human race into extinction.

Evolution has granted us our strongest instinct: survival. Instinctively we are in a never-ending war with nature, aiming to prolong our existence. In the abstract, the field of medicine solely exists for this purpose. Therefore, instinctively we will either try to eliminate the existential threat that ASIs might pose against us when we face the threat itself or try to eliminate a potential threat prematurely and in so doing cause our own extinction.

3.2. Reshaping perception on law

We may be living in the dawn of the age of artificial intelligence today. Consequently, the legal landscape surrounding our lives will require rethinking, as the case was with every big leap in technology. The industrial revolution brought conveyor belts and mechanical manufacturing processes operated by workers for longer and longer hours, which ended in myriad clashes between proletariat and employers. Hence, we developed labour laws, bringing a humanitarian minimum standard for the workers that were suffering from extreme working conditions. Similar legislative efforts followed each time when technologies required us to adapt new paradigms they introduced, technologies such as electricity, telegraph, telephone, railroad, automotive, television, and computers and so on. . . Below we will seek answers to some exemplary questions as to how AI might reshape our thinking, in terms of certain matters of current and prospective law.

3.2.1. Liability on damages

There are very few laws or regulations that address the challenges raised by AIs, and no courts appear to have developed standards so far, addressing who is legally responsible if an AI causes harm. The diversity and richness of individuals and firms that participate in the creation of an AI will make it difficult to identify the persons under liability. Certain technologies used in the development of an AI may date back to years before such AI is developed. Further, the developers of such technology may never have thought that one day, someone might incorporate their creation into any AI system. In such circumstances, it would be unfair to hold the developer of such technology responsible for a possible tort.

National and international laws do not recognize AI as a legal person. Therefore, current legal systems cannot hold them liable for the damages they might cause. However, what if an AI was fully autonomous and aware of its actions, causing harm knowingly and willingly?

This brings us back to the debate on consciousness. A conscious AI should naturally be liable for its actions. However, how can that be possible if we keep refraining from coming up with an adequate definition of what an AI is as far as legal ‘beings’ are considered? Should we ascribe legal personhood to them? (Paulius et al., 2015).

3.2.2. Intellectual property

IP law and its application places human initiative at its core. Berne Convention of 188623 requires an ‘author’ and an ‘artistic work’ to begin talking about intellectual property. While there is no limitation as to what form a ‘work’ can assume as long as humans can perceive it, an author must be a ‘human’. A San Francisco court applied and materialized this concept in 2015 by deciding in a lawsuit by PETA, the renowned organization defending animal rights, against David John Slater, a professional photographer, that a macaque money cannot own copyright to a selfie it took using the photographer’s camera (Kravets, 2016). What about AIs though? Can they own copyrights to the artistic works they create? Should law consider them as ‘individuals’?

3.2.3. Copyright and AI

Currently, a handful of AI applications are capable of producing works that resemble ‘art’, such as Deep Dream and the Cybernetic Poet.

Google’s® researchers developed DeepDream® to create a human-like image recognition software to identify certain things through mimicking human cognitive abilities. DeepDream uses Google’s artificial neural networks protocol to discern and process images of things to learn what they look like, such as a cat.

Google’s developers taught DeepDream what a cat looks like by showing millions of images of cats. Then they put DeepDream’s learning and identifying abilities to test by asking it to identify cats in pictures with cats and if found amplify them, introducing a feedback loop to work on. Then the developers introduced a random image to DeepDream and asked it to enhance the image in such a way as to elicit a particular interpretation. This method enabled the developers to understand whether DeepDream understood the essence of the things it learns. As a result, DeepDream searched in the images provided for all the things the developers trained it to recognize and when it found the tiniest bit of reference, it enhanced the relevant reference to make it look like the thing it found similar. The resulting images were surprisingly close to works of art. Few predicted this phenomenon, including DeepDream’s developers.24

Ray Kurzweil developed a poem software in mid-80s, a computer-implemented method of generating a poet personality that reads poems and generates analysis models to build its personality, and ultimately writes poems; the ‘Cybernetic Poet’. Cybernetic Poet is “provided with an input file of poems written by a human author or authors. It analyses these poems and creates a word-sequence model based on the poems it has just read. It then writes original stanzas of poetry using the model it has created.” (Bridy, 2012)

Now, who owns the copyrights of the artistic works created by these AIs?

As explained, current law cannot vest ownership of the copyrights to an AI, as it is not ‘human’. However, the laws of the United Kingdom make express provision for copyright in computer-generated works and introduce the following definition: ‘works generated by a computer in circumstances such that there is no human author’.25 The copyright in such works under UK law vests in ‘the person by whom the arrangements necessary for the creation of the work are undertaken’. Concordantly, Irish Law adopts the same principles.26 However, the UK and Irish approaches to the issue surrounding copyright ownership of computer-generated works and not the works of an AI. Therefore, they overlook the possibility of ‘non-human’ copyright ownership, ruling out the possibility of an AI that develops its own creative abilities. Who will have the ownership then?

3.3. Regulate and dominate?

A regulatory oversight and governmental intervention is a need when the development of AI is considered.27 It is not common to hear a Silicon Valley entrepreneur who operates on the frontiers technological advancement, urge governments to directly intervene with a developing technology in the hope of preventing humanity to do ‘something stupid’. When such thing happened in October 2014, it created a ripple effect and caused ‘The Great AI Panic of 2015’ (Sofke, 2015), which eventually led an institution called ‘Future of Life Institute® (FLI)’ to issue an open letter signed by Elon Musk, Stephen Hawking, hundreds of AI researchers in addition to many individuals representing U.S. government (Russel et al., 2015). FLI urged expanded research on how to contain AI systems within the walls of human benefit, including premature regulation. However, FLI used statements such as ‘AI systems must do what we want them to do’, ‘We should identify research directions that can maximize societal benefits’ and ‘AI super-intelligence will not act with human wishes and will threaten humanity’ while providing a research roadmap for AI researchers.

While the ‘we’ hints at a desired ownership over a technology under development (i.e. AI) and the ‘we’ implies superiority over ‘others’ in determining how a technology will be socially beneficial for humanity. It also begs the questions, ‘Who are you to claim that you have the capacity to force your desires over the entire human race, and who are you to claim that you can decide what is socially beneficial for us?’ Stating that an ASI will definitely be against the humanity’s welfare is an unexpectedly ignorant claim, allegedly coming from some of the greatest minds on Earth.

We experienced this line of thought when the Internet reached the masses, disrupting the status quo by lifting the boundaries of communication and information exchange and blurring the sense of control over disseminated information and access to such. The idea of an open interconnected network of networks that is not in anyone’s control or under any jurisdiction challenged lawmakers, policy makers and judiciary bodies and it still does. We have still been unable to set out universal rules on Internet (except DNS policies, where all stakeholders over Internet govern these policies through ICANN, a non-governmental organization) for almost 60 years. It would be very naïve to think that we can regulate AI policies, while AI is still in its infancy.

There is almost a consensus within the scientific AI community that definitive predictions on the future of ASI are impossible at this stage, simply because we are so far from creating an ASI, let alone understanding its implications.

3.3.1. Current and prospective regulatory efforts

Trying to anticipate ASI’s desires from where we stand now in terms of AI development is very similar to a chimpanzee trying to anticipate our motives when we crush an onion to remove its skin. Therefore, aiming to establish regulations to prevent ASIs from obliterating us is a hopeless endeavour. However, this line of thought may eventually lead regulators to prevent AI research from developing an AGI, fearing that it will break free from the chains of our capacity and become an ASI by itself. For example, John FrankWeaver, an attorney working in the field of AI law, praised the regulators at California when they intervened with Google’s self-driving cars and required test drivers to be present in these cars. He even claimed that this as a ‘wonderfully swift governmental response to autonomous technology and artificial intelligence’ while further supporting four states (Mississippi, Florida, Nevada and California) for passing restrictive regulation on autonomous cars that are not even on the market yet (Weaver, 2014).

3.3.1.1. Legislative efforts for autonomous vehicles. Nevada is the first U.S. state to enact a legislation authorizing the operation of autonomous vehicles in 2011 and was then followed by six other states, with many other states in still pending status with reference to their respective autonomous vehicle legislations. Tennessee among those who did enact such legislations stands out with its enabling and refreshing legislation wherein it prohibits local governments from banning the use of motor vehicles equipped with autonomous technology (Legislatures, 2016).

Throughout the world, legislators are working to incorporate autonomous (driverless) vehicles into their legislations to allow this thriving technology bloom and develop further, which brings hope.

The Convention on Road Traffic,28 of the United Nations, ratified by 73 countries, is in the process of amendment to allow automated vehicles on roads in many countries. European Road Transport Research Advisory Council published the roadmap for automated driving for Europe.29 German Federal Highway Research Institute published a report on the status of German legal landscape pertaining to vehicle automation technologies, indicating the areas of improvement on research, legislation and involvement of government agencies.30 Netherlands, Sweden, Japan and many other developed countries are actively working on improving the conditions of economic and legislative environment to enable swift development and consequently to reap the benefits of being involved in the forefront of innovative technologies.

While governments are honing in on preparing the legislative grounds for the operation of autonomous vehicles, academia adopts a wider approach and handles the concept in a wider manner, and works on determining the adequate policies for robotics and AI.

3.3.1.2. The RoboLaw project. The main objective of the RoboLaw project (“Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics”) is to understand the legal and ethical implications of emerging robotic technologies and to uncover whether existing legal frameworks are sufficient in light of the rapid expansion of robotics technologies.31

The project was launched in March 2012 and funded by the European Commission (Paulius et al., 2015). The project produced the “Guidelines on Regulating Robotics”, which was then presented to the European Commission, to create the legal framework surrounding the development of robotic technologies in Europe.

The RoboLaw Project considered industrial robots, domestic robots, care robots, medical and surgery robots, autonomous vehicles, and humanoids/animaloids.The report discussed five essential legal areas for robotics: (i) health, safety, consumer, and environmental regulations; (ii) liabilities; (iii) intellectual property rights; (iv) privacy; and data protection and (v) capacity for legal transactions (Anon, 2015).

3.3.1.2.1. Health, Safety, Consumer and Environmental Regulation. The report identifies that common usage of robotics in hospitals, homes, commercial areas and our daily lives will require a new wave of legislations to cope with the prospective health and safety matters.

3.3.1.2.2. Liability. The report argues that imposing substantial liability on manufacturers, owners or users of robots for damages caused to third parties may increase safety while inducing wider social acceptance of robots. However, the report also argues that such approach on a liability regime may result in the displeasure of tech industry, consumers and, in the end, the general public, and may slow down the development of AI and robotics technologies. Therefore suggests a balanced approach between the interests of manufacturers, users, and third parties, and between risk regulation and stimulation of innovation, to encourage research, innovation and experimentation on these technologies, for increasing welfare in health, transport, commerce and other areas of business.

3.3.1.2.3. Intellectual Property Rights. RoboLaw Project indicates the lack of legal provisions that specifically apply to robotics. RoboLaw Project states that further research would be beneficial to determine whether the current application of intellectual property rights sufficiently meets the needs of the robotic industry and society.

3.3.1.2.4. Privacy and Data Protection. The RoboLaw Project suggests implementation of legal requirements into the robot’s software and interface through the ‘privacy by design’ approach, such as data security through data encryption and data access control in order to comply with the data protection requirements.

3.3.1.2.5. Capacity for Legal Transactions. The report stresses the lack of legal personality of robots and indicates that robots are seen as ‘mere tools’ to carry out commands that can, directly or indirectly, be attributed to human beings. Consequently, this approach requires the legal responsibility for robot actions to rest with their human ‘masters’.

It is possible to attribute legal personality to robots through legislative effort. Non-humans such as corporations, associations, and foundations gain their legal personalities through registration. The registration principle could be extended to robots and AIs (including requirements how robots can prove their registered identity); the capability of owning property is less easy to create, although legal constructions could be devised to accommodate this.

The report concludes with indicating that if these issues concerning legal personality are resolved at a certain point in time, more practical requirements and rules pertaining to legal acts will come into play, such as implementing legal conditions into the machines to make it possible for them to enter into a contract.

Lawmakers need to familiarize themselves with the potential benefits of AIs. Strict rules may prevent humans from the possible damages of AIs. However, these rules will also dampen possible improvements. Therefore, lawmakers should consider the balance between protection of humanity and development in technology.

4. Conclusion

When aiming to regulate currently non-existent technologies, we must avoid this approach at all costs. Putting restrictions on developing technologies based on our personal presumptions might indeed help us to avoid extinction at the hands of ‘evil robots’, but it might also cause our extinction due to natural reasons, such as evolution by making it harder for the human race to use technology to adapt.

Based on the statements of Elon Musk, SteveWozniak, Bill Gates, Bill Joy, Stephen Hawking and FLI’s open letter, it is clear that what they all fear is an ‘unfriendly AI’ and what they all want is a ‘friendly AI’ in the abstract.

The terms ‘friendly’ and ‘unfriendly’ do not refer to a personal trait of an AI system. These terms refer to whether the actions of an AI will have a positive or a negative impact on humanity (Urban, 2015). This is because AIs are computers and they do not have human values. We tend to anthropomorphize32 AI and attribute them with our moral values such as ‘good and evil’, ‘moral and immoral’ that are formed by our consciousness. These attributes developed only after thousands of years of social interaction. AIs will not share these human traits unless we specifically create them to do so. They operate on a task and goal oriented manner. To illustrate this point, for instance, there is an AGI, whose main task is to ensure that trees in a certain pine tree plantation are under protection from alien spores to keep the tree DNA as pure as possible. We should not be surprised when such an AGI takes drastic measures as far as obliterating the entire flying bug population in the area. One who is unaware of the goals of this AGI might easily label it as ‘evil’ and a ‘danger to humanity’ as he/she has no preconception on what the AGI’s motives or goals were. Similarly, a chimpanzee fearing that the crushing of an onion is a sign of aggression might attack us. Ironically, this view is very similar to the perspective of those who propose premature regulation of AIs.

#### Regs block innovative start-ups AND make advanced neural nets infeasible

Daniel Castro 19, Vice President at the Information Technology and Innovation Foundation (ITIF) and Director of ITIF's Center for Data Innovation, M.S. in Information Security Technology and Management from Carnegie Mellon University, B.S. in Foreign Service from Georgetown University, and Michael McLaughlin, “Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence”, Information Technology & Innovation Foundation, 2/4/2019, https://itif.org/publications/2019/02/04/ten-ways-precautionary-principle-undermines-progress-artificial-intelligence

HOW POLICIES BASED ON THE PRECAUTIONARY PRINCIPLE IMPACT AI

Policies based on the precautionary principle can impact AI in several ways. They can make it more expensive to develop AI, limit the testing and use of AI, and even ban certain applications. Clearly nations have the right to impose any regulations they chose (assuming they do not violate World Trade Organization rules or other global treaty obligations). But they should not delude themselves into believing that regulatory regimes based on the precautionary principle will not limit increased productivity, competitiveness, and innovation.

To provide a more detailed discussion of the negative effects policies based on the precautionary principle can have on AI, the following section analyzes the effects of policies discussed earlier in this report. In many cases, these policies have multiple negative effects on AI.

1. Slower and More Expensive AI Development

Policies based on the precautionary principle both slow and make the development of AI more expensive. For example, if all fifty U.S. states had laws such as New York’s, which requires autonomous vehicle firms to perform road testing under the paid supervision of police, testing such vehicles would be more expensive. Moreover, proposals to require even non-medical algorithms to undergo pre-market trials would hurt the development of AI because such trials are time-consuming and expensive. Such proposals may also make AI systems that use machine learning, and thus may change frequently and need more testing, significantly less viable because such systems could constantly need to go through a new approval process.96 Finally, policies that increase the cost of developing AI would likely discourage innovation in AI by creating a substantial barrier to entry for startups that lack sufficient funding to cover the cost of proving their AI system is safe. For example, the GDPR has dampened investment in European technology startups and led to a 30 percent decrease in the market share of small online advertising firms that lack the resources to easily comply with the regulation.97

Restrictions on one AI technology can also limit ways to develop another AI technology. For example, researchers in Germany are using drones hovering hundreds of meters above highways to record the movements of vehicles. This data can help develop simulations to test autonomous vehicles; such simulations are important tools for improving the safety of autonomous vehicles because otherwise they would need to travel billions of miles for safety validation.98 While this novel method of collecting data to validate the safety of autonomous vehicles may or may not prove valuable, implementing it in the United States would be would be difficult to do at scale until the FAA implements its new rules that allow out-of-sight drone flights and flights over people.99

2. Less Innovation

AI will spur innovation so policies that limit the development of AI will limit innovation.100 For example, proposals to ban or limit the introduction of autonomous vehicles would also limit the generation of new businesses, business models, and ways to do deliver services through the “passenger economy.” The passenger economy, a term coined by Intel and research firm Strategy Analytics, “is the economic and societal value that will be generated by fully autonomous…pilotless vehicles.”101 The firms envision a world where a significant portion of vehicle ownership is replaced by fleets of autonomous vehicles that provide on-demand transportation. Productivity would also increase as autonomous vehicles free employees to work during their commutes and autonomous trucks to operate more efficiently. The firms estimate the value of this economy could be $7 trillion by 2050.102 Nations that ban autonomous vehicles will not experience the benefits of such an economy.

3. Lower-Quality AI

There is often a negative correlation between making an AI system more explainable and its accuracy.103 As a result, any policies that require AI to be explainable could lead to less accurate AI. For example, researchers at Mount Sinai Hospital in New York developed an AI system called Deep Patient that can predict whether a patient is contracting any of a wide variety of diseases.104 The researchers trained Deep Patient on the health data from 700,000 patients, using hundreds of variables, such as test results, which allow it to predict diseases such as schizophrenia—which doctors struggle to predict—extremely well.105 Even though its operators can verify its accuracy by measuring outcomes, such as if a person is developing a disease, it is difficult for its own developers to know why it made a particular decision.106

Many sophisticated forms of AI pose a similar problem. Developing an AI system capable of explaining itself or justifying its decisions is an incredibly challenging technical feat, so much so that the U.S. Defense Advanced Research Projects Agency (DARPA) devoted $75 million in 2017 to research how AI could achieve it.107 Some groups are skeptical that requiring explainability would chill innovation. They cite DeepMind, a British company owned by Google parent-company Alphabet, developing an AI system in 2018 that can analyze eye scans to predict diseases while also providing doctors a map of the features of disease it sees, such as hemorrhages.108 However, the fact that one of the world’s leading AI companies could achieve a form of explainability in a system it worked on for nearly two years is not evidence that all other operators should or would be able to achieve explainability for their AI easily.109 To be clear, it is legitimate for companies, such as IBM, to create internal requirements for AI explainability.110 Requiring all firms to meet such a standard, however, would create a barrier to adopting AI, because not all AI systems are alike and not all businesses have a similar level of expertise.

Nonetheless, it is important for AI operators to continually assess their AI system’s accuracy to ensure it is generating or predicting the correct outcomes. The other option is to allow only AI applications that operators can explain; this would lead to AI systems that consider fewer variables and that use simpler algorithms to make decisions. In turn, this would reduce the effectiveness of AI that can generate significant impacts such as identifying a terminal illness before a doctor can.

#### It nukes R&D at the small business and individual levels---they’re key

Dr. Jeremy Straub 21, PhD, Assistant Professor in the North Dakota State University Department of Computer Science and NDSU Challey Institute Faculty Fellow, “Would Regulation Prevent AI From Becoming an Evil Overlord?”, Dakota Digital Review, 10/1/2021, https://dda.ndus.edu/ddreview/would-regulation-prevent-ai-from-becoming-an-evil-overlord/

WHO DOES REGULATION REALLY PROTECT?

Achieving most of these benefits will require a lot more research and development. Regulations that make it more expensive to develop AIs or prevent certain uses might delay or forestall those efforts. This is particularly true for small businesses and individuals—key drivers of new technologies—who are not as well equipped to deal with regulation compliance as larger companies.

In fact, the biggest beneficiary of AI regulation may be large companies that are used to dealing with it, because startups will have a harder time competing in a regulated environment. Even ambiguity regarding regulation and what aspects of AI are regulated may be problematic, as it may cause people to avoid innovation to avoid risking inadvertent ensnarement by vague regulations and potential penalties.

Humanity faced a similar set of issues in the early days of the internet. But the United States actively avoided regulating the internet to avoid stunting its early growth.[39] Elon Musk’s PayPal and numerous other businesses helped build the modern online world while subject only to regular human-scale rules, like those preventing theft and fraud. Similarly, no special rules were rolled out to govern early software businesses, such as Microsoft, in their burgeoning years, that have gone on to become industry titans.

### 2NC---Gradualism

#### Users will naturally demand sufficient transparency to allow stepwise controls under the existing legal structure---that completely caps existential risk without jumping the gun on broad regulation

Chris Reed 18, Professor of Electronic Commerce Law at Queen Mary, University of London, LLM from the University of London, “How Should We Regulate Artificial Intelligence?”, Philosophical Transactions of the Royal Society B, Volume 376, Issue 2128, 9/13/2018, https://royalsocietypublishing.org/doi/10.1098/rsta.2017.0360

9. Masterly inactivity?

The analysis in this paper suggests that some form of regulation will be needed for some uses of AI. But does that mean that we need to regulate now?

I argue that the answer is a qualified ‘No’. Responsibility for autonomous vehicles is clearly problematic, and the uncertainty about the current application of the law is likely to inhibit their adoption unless the position is clarified, as the UK and other lawmakers are currently doing. The use of technology in medicine is already regulated by the profession, and that regulation will certainly be adapted piecemeal as new AI technologies come into use. There are probably other high-risk uses of AI which will demand some level of legal and regulatory change. But, all these areas are likely to be regulated already, as is the case for road vehicles and medicine, so the existence of current regulation might provide a useful guideline about where to focus the immediate regulatory effort.

So far as regulating the rest of life is concerned, I have attempted to show that transparency will be enough to allow the current legal and regulatory regime to produce at least adequate answers. Because that regime also provides sufficient incentives for users to demand and producers to develop transparency of AI decision-making, there is no need to panic. A ‘wait and see’ approach is likely to produce better long-term results than hurried regulation based on, at best, a very partial understanding of what needs to be regulated.

#### Iterative legal development is inevitable---at each step, AI will be matched with tailored controls

Adam Thierer 16, MA in International Business Management and Trade Theory from the University of Maryland, BA in Journalism and Political Philosophy from Indiana University, Former President of the Progress & Freedom Foundation, Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom, Revised and Expanded Edition, p. 41-66

Most notable in this regard is the scathing social criticism of the prolific techno-skeptic Evgeny Morozov, who goes so far as to argue that the very term “the Internet” is a meaningless construct.20 He engages in a sort of radical deconstructivism that suggests we are all somehow being fooled into thinking the Internet is as important or meaningful as most of us, quite rationally, believe it is. Morozov also rails against what he regards as the irrational exuberance of digital innovators, who supposedly believe technology can solve all the world’s hard problems. He refers to this as “solutionism” and castigates all those who would engage in a “mindless pursuit of this silicon Eden” or “romantic and revolutionary” thinking about how new technology might improve our lives.21 The critiques set forth by the latest crop of critics have become even more specialized, zeroing in on emerging technologies such as robotics,22 artificial intelligence,23 sensors,24 and the Internet of Things.25 Again, the concerns range from social (e.g., privacy, safety, and security) to personal (e.g., impact on learning and concentration) to economic (e.g., fears about automation and job dislocation). And it is not unusual to also hear a fair share of end-of-world dystopian scenarios thrown around in many of their books and essays, including Terminator-inspired tales of killer robots destroying humanity.26

The critics often fail to devise a coherent political or regulatory agenda for countering what they see as an overreliance on technology. However, when they do come clean about their policy intentions, they are usually calling for quite radical policy interventions, often aimed at imposing sweeping political control over the future course of technological innovation.27

B. ANSWERING THE TECH CRITICS: THE CASE FOR “RATIONAL OPTIMISM”

The problem with all these critics’ arguments is that they overestimate the dangers of new innovations while ignoring, or at least greatly underplaying, the importance of technological innovation for economic and social progress.28 And perhaps the most important shortcoming of these techno-critics, as I’ll discuss in greater length in chapter IV, is that they consistently fail to appreciate how well humans adapt to technological change. In fact, they almost universally ignore how quickly we learn to cope with changes that—while challenging in the short term—ultimately come to be an accepted, and usually enriching, part of our lives.29 Although they are rarely as direct about saying it as Morozov is, the work of some tech critics implies that all this modern innovation isn’t necessary, or at least that there’s just too much irrational exuberance about its potential.

It’s easy for some modern technological critics to dismiss the wild-eyed enthusiasm of some creators because, at times, those innovators or others can overstate the potential of any given invention. When Pollyanna-ish pundits make sweeping claims about how any particular new technology will “change everything” or seemingly solve all the world’s problems, the critics are right to call them out for such statements.

But that criticism can go too far and ignore the fact that, as James Surowiecki observes, “[i]n the delusions of entrepreneurs are the seeds of technological progress.”30 It is hard to believe, for example, that the world would really be a better place if it was completely devoid of the “romantic and revolutionary” thinking that Morozov and other critics deride. We need not always support the bullish enthusiasm of all modern entrepreneurs to nonetheless appreciate how their ongoing efforts to find solutions to hard problems can often yield very beneficial results—or even just powerful lessons following their failures.

This more practical disposition toward technological experimentation and change is what author Matt Ridley calls “rational optimism.”31 At a macro level, the rational optimist is generally bullish about the future and the prospects for humanity but is not naive about the challenges associated with technological change. At the micro level, the rational optimist seeks practical solutions to intractable problems through ongoing trial-and-error experimentation, but is not wedded to any one process or particular technology to get the job done.

This is the approach seen in the works of Herman Kahn,32 Julian Simon,33 F. A. Hayek,34 Ithiel de Sola Pool,35 and especially Aaron Wildavsky and Virginia Postrel, whose work was discussed earlier. These “dynamist” thinkers express optimism about the role technology plays in advancing social and economic progress, but their optimism is always rooted in empiricism and rational inquiry, not blind faith in any particular viewpoint or ideology. Rational optimists don’t hold an unthinking allegiance to technology as an autonomous force or savior to all of civilization’s woes. Indeed, the blueprint that rational optimists offer is not utopian but anti-utopian: precisely because difficult problems defy easy solutions, we should look to devise a plurality of strategies to tackle them. New technological innovations might be among those strategies, but they are not the only ones we should rely on. Ongoing experimentation is the key to unlocking knowledge and prosperity.36

Importantly, rational optimists would never discourage the entrepreneurial dreaming and daring that so many modern tech critics deride. While Morozov and other critics might lambast those “romantic and revolutionary problem solvers,” the truth is that the world is a better place because such people exist. Much of their entrepreneurial activity will yield socially beneficial results. Equally as important, however, is the fact that it will also produce many failures, but society will then learn from those mistakes and improve future experiments accordingly.

The goal is not to “save everything” with “the folly of technological solutionism,” as Morozov worries. Rather, it is to seek to solve‑some‑problems through the application of practical knowledge to social and economic challenges through incessant experimentation with the new and different approaches to those problems.37 But rational optimists will not shy away from the fundamental truth that a symbiotic relationship exists between technological innovation and human flourishing. That connection, as noted next, is why the critics’ complaints must be met with a full-throated response.

C. THE CONNECTION BETWEEN INNOVATION, ECONOMIC GROWTH, AND HUMAN FLOURISHING

Before we consider the profound benefits associated with innovation, we should try to define the term. Of course, defining “innovation” is notoriously difficult,38 almost as challenging as settling on a good definition of “technology” itself.39 The Organisation for Economic Co-operation and Development (OECD) rather dryly defines innovation as “the implementation of a new or significantly improved product (good or service), or process, a new marketing method, or a new organizational method in business practices, workplace organisation or external relations.”40 But, as is often the case with other attempted definitions of the term, the OECD caveats its definition by noting how “[t]his broad definition of an innovation encompasses a wide range of possible innovations” and that narrower and more nuanced definitions are available.41

W. Brian Arthur, author of The Nature of Technology, argues that the problem with trying to explore the concept of innovation directly is that “the idea is too diffuse, too nebulous, for that to be useful.”42 Despite that warning, he continues on to explain how

[i]nnovation has two main themes. One is [a] constant finding or putting together of new solutions out of existing toolboxes of pieces and practices. The other is industries constantly combining their practices and processes with functionalities drawn from newly arriving toolboxes— new domains. . . . The result is new processes and arrangements, new ways of doing things, not just in one area of application but all across the economy.43

More concisely, in their book Innovation Economics, Robert‑D. Atkinson and Stephen J. Ezell define innovation as “the development and widespread adoption of new kinds of products, production processes, services, and business and organizational models.”44 What these and most other definitions of innovation share in common, then, is a focus on new and better ways of doing things and, in particular, new ways of satisfying human wants and needs. Thus, even if its precise definition proves elusive, what is most crucial about the process of innovation is that it serves as a means to an end: it helps drive progress and human flourishing. “Innovation is more than the latest technology,” notes Sofia Ranchordás, a resident fellow at Yale Law School, “it is a phenomenon that can result in the improvement of living conditions of people and strengthening of communities. Innovation can be technological and social, and the former might assist the latter to empower groups in ways we once thought unimaginable,” she observes.45

The endless search for new and better ways of doing things drives human learning and, ultimately, prosperity in every sense— economic, social, and cultural. The pessimistic critics of technological progress and permissionless innovation have many laments, but they typically fail to consult the historical record to determine how much better off we are than our ancestors.46 And that record is unambiguous, as Robert Bryce explains in his recent book, Smaller Faster Lighter Denser Cheaper: How Innovation Keeps Proving the Catastrophists Wrong:

The pessimistic worldview ignores an undeniable truth: more people are living longer, healthier, freer, more peaceful, lives than at any time in human history… [T]he plain reality is that things are getting better, a lot better, for tens of millions of people around the world. Dozens of factors can be cited for the improving conditions of humankind. But the simplest explanation is that innovation is allowing us to do more with less.47

“Doing more with less” drives greater economic efficiency, expands the range of goods and services available, and generally lowers prices.48 This raises our overall standard of living over the long term.49

Indeed, there exists widespread consensus among economic historians and scholars that, as the Cato Institute’s Brink Lindsey asserts, “the long-term future of economic growth hinges ultimately on innovation.”50 Countless economic studies and historical surveys have documented the positive relationship between technological progress and economic growth. A 2010 white paper from the US Department of Commerce revealed that “[t]echnological innovation is linked to three-quarters of the Nation’s post-WW II growth rate” and continued on to note that,

[a]s it fuels economic growth, innovation also produces high-paying jobs. Recent studies by the Federal Reserve show that innovation in capital goods is the primary driver of increases in real wages. Without innovation, wages would be much lower.‑Additionally, across countries, 75% of differences in income can be explained by innovation-driven productivity differentials.51

These findings are reflected in many other major economic studies on the factors that drive economic growth. For example, two major economic surveys from 2003 and 2006 found that technological progress accounts for 30–34 percent of growth in Western countries.52 And economists estimate that differences in technological adoption patterns account for 80 percent of the difference between rich and poor nations.53

Of course, just because the historical evidence linking innovation and long-term growth reveals an unambiguous and undeniable relationship, the short-term disruptions caused by technological change won’t be any easier to swallow for some individuals, businesses, or public policymakers.

This is why attitudes toward innovation and entrepreneurship are so important. Progress-oriented policy requires a general openness to constant change and the “creative destruction” that Austrian-born economist Joseph Schumpeter famously spoke of in the 1940s, when he explained how cascading waves of continuous change, or what he described as the “perennial gales of creative destruction,” were what spurred innovation and propelled an economy forward.54 As my Mercatus Center colleague Jerry Ellig has explained it, in the Schumpeterian paradigm, “firms compete not on the margins of price and output, but by offering new products, new technologies, new sources of supply, and new forms of organization.”55

The Schumpeterian paradigm and other “dynamic competition” models best capture the nature of competition and innovation in today’s digital world.56 The Schumpeterian model explains why some tech companies can gain scale so rapidly only to stumble and fall with equal velocity.57 Digital Davids are constantly displacing cyber-Goliaths.58 Social and economic risk takers and innovators are constantly shaking things up in the digital economy and bringing about equally seismic disruptions throughout our culture.59

New disruptions flow from many unexpected quarters as innovators launch groundbreaking products and services while also devising new ways to construct cheaper and more efficient versions of existing technologies. The more this cycle repeats, the more likely economic growth becomes. But the Schumpeterian model also explains why technological innovation can be so gut-wrenching and generate so much opposition in the short term.

Indeed, it’s amazing to think about all the once-mighty tech titans that ruled their respective sectors, only to be rapidly displaced by smaller start-ups a short time later.60 For some, the velocity of their downfall was precipitous and fatal. Other times their decline and fall was gradual and incomplete as the shells of the old companies remain in existence even as their cores have been hollowed out. Consider a few examples:

* IBM: “Big Blue” was once synonymous with computing itself. IBM dominated the mainframe computer marketplace and kept antitrust officials in a 13-year tizzy. But both‑IBM and the government weren’t paying attention to the personal computing revolution, which abruptly kicked IBM off its perch and utterly decimated its business and shareholder value throughout the 1980s. While it reinvented itself later and rebounded, it is a shadow of the company that once ruled the computing marketplace.
* Kodak: The postwar generation had “Kodak moments” and the film and camera giant’s importance was significant enough that even singer Paul Simon begged, “Mama, don’t take my Kodachrome away.” But the combination of digital photography, online photo storage, and home printing would eventually wipe out Kodak’s market dominance, even though the firm had seen much of the change coming. Its failure to adapt led the firm into bankruptcy in 2012.61
* Sony: For those coming of age in the early and mid- 1980s, “Walkman” was synonymous with any portable music device. Sony had created a product that everyone wanted and all its competitors were forced to copy. A generation later, the device had lost much of its appeal— and whatever market dominance Sony once gained from it. By the late 1990s, digitized music and the rise of MP3 players meant that Apple and others would rapidly eat away at Sony’s once-dominant position. Although the company rebounded and remains a major player in video games and other consumer electronics sectors, it is not the feared juggernaut it once was.
* Atari: For the first generation of video gamers, Atari was the name of the game. It dominated the home console market in the late 1970s. A few years later, it was “game over” for the company, primarily because of Nintendo’s growing dominance of the console market in the late 1980s. While Nintendo would last longer and indeed is still with us, the firm faces vigorous competition from other platforms, including the unexpected rise of smartphones as a major gaming platform.
* MySpace: While Facebook dominates discussions about social networking today, it’s already easy to forget that just a few years ago almost everyone expected MySpace to rule social networking for a long time to come. That concern over MySpace’s hegemony peaked shortly after Rupert Murdoch and News Corp. bought the company in 2005 and led critics like Victor Keegan of the United Kingdom’s Guardian newspaper to ask, “Will MySpace Ever Lose Its Monopoly?”62 A short time later, however, MySpace lost its early lead and became a major liability for Murdoch—he paid $580 million for the company in 2005, but sold it for only $35 million in June 2011.63
* Mobile phones: The mobile phone handset and operating system (OS) marketplace has undergone continuous change over the past 15 years and is still evolving rapidly. When cellular telephone service first started taking off in the mid-1990s, handsets and mobile operating systems were essentially one in the same, and Nokia and Motorola dominated the sector with fairly rudimentary devices. The era of personal digital assistants—more commonly known as PDAs—dawned during this period, but mostly saw a series of overhyped devices, such as Apple’s “Newton,” that failed to catch on. In the early 2000s, however, a host of new companies and devices entered the market, many of which are still major players today, including LG, Sony, Samsung, Siemens, and HTC. Importantly, the sector began dividing into handsets versus OS. Leading mobile OS makers have included Microsoft, Palm, Symbian, BlackBerry (RIM), Apple, and Android (Google).

The sector continues to undergo constant change. Palm smartphones were wildly popular for a brief time and brought many innovations to the marketplace.64 Palm underwent many ownership and management changes, however, and rapidly faded from the scene.65 Similarly, RIM’s BlackBerry was the dominant smartphone device for a time, but it has recently been decimated.66 BlackBerry’s roller-coaster ride has left it “trying to avoid the hall of fallen giants,” in the words of an early 2012 New York Times headline.67 Although the company once accounted for more than half of the American smartphone market, today its share has slipped into the single digits.68 Microsoft also had a huge lead in licensing its Windows Mobile OS to high-end smartphone handset makers until Apple and Android disrupted its business. It is hard to believe now, but just a few years ago the idea of Apple or Google being serious contenders in the smartphone business was greeted with derision, even scorn.

Famously, many commentators denigrated Apple’s entry into the smartphone business because many industry analysts believed the market was mature.69 Just a few years later, Nokia’s profits and market share plummeted,70 and Google purchased the struggling Motorola. Meanwhile, Palm is dead and Microsoft is struggling to win back market share lost to Apple and Google. “The violence with which new platforms have displaced incumbent mobile vendor fortunes continues to surprise,” says wireless industry analyst Horace Dediu.71

In each of these cases, Schumpeterian change has brought us many new goods and services that have improved our overall standard of living. But precisely because disruption of this sort unsettles so many traditional businesses, sectors, and professions, the shortterm opposition to change will always be vociferous.

Nonetheless, the vital lesson here is perfectly summarized by Daron Acemoglu and James A. Robinson, authors of Why Nations Fail, when they conclude: “Sustained economic growth requires innovation, and innovation cannot be decoupled from creative destruction, which replaces the old with the new in the economic realm and also destabilizes established power relations in politics.”72 When public policy discourages risk-taking and actively regulates to disallow permissionless innovation, the result is less entrepreneurialism, diminished competition, fewer consumer choices, and stagnated economic growth.73 The following case study of Europe’s declining global competitiveness in the digital marketplace over the past 20 years makes that abundantly clear.

D. THE REAL-WORLD IMPACT OF PERMISSIONLESS INNOVATION

Let’s get even more concrete about how creative destruction plays out in the real world and how permissionless innovation affects the standard of living for different populations.74 To do so, consider this question posed by James B. Stewart in a summer 2015‑New York Times‑column: “Why hasn’t Europe fostered the kind of innovation that has spawned hugely successful technology companies?”75 That‑question helps frame the importance of the debate between permissionless innovation and the precautionary principle.

Since the rise of the commercial Internet in the mid-1990s, the United States and the European Union have adopted starkly different visions toward the digital economy and innovation policy more generally.76 This is particularly true as it relates to online advertising and the data collection practices that have powered digital commerce over the past two decades.77 Beginning in 1995 with the adoption of its “Data Protection Directive,” the European Union has instituted highly restrictive policies governing online data collection and use.78 The EU’s approach has been shaped by precautionary principle thinking at every turn, based largely on concerns about privacy and data security. Combined with “a deeply ingrained fear of failure that is a bigger impediment to entrepreneurship on the Continent than in other regions,”79 this general aversion to change has greatly discouraged innovation in Europe.80 Indeed, attitudes toward risk and failure account for the significant differences in US and EU policy and help unlock the mystery of why American tech firms have grown so much faster and bigger than European firms.81 German economist Petra Moser notes that Europeans are “trying to recreate Silicon Valley in places like Munich, so far with little success,” because “[t]he institutional and cultural differences are still too great” and “[i]n Europe, stability is prized” above all else, she says.82 In his recent Times essay on this transatlantic clash of visions, Stewart noted that [o]ften overlooked in the success of American startups is the even greater number of failures. “Fail fast, fail often” is a Silicon Valley mantra, and the freedom to innovate is inextricably linked to the freedom to fail. In Europe, failure carries a much greater stigma than it does in the United States.83

Moreover, he notes, “Europeans are also much less receptive to the kind of truly disruptive innovation represented by a Google or a Facebook.”84 What European regulators fail to appreciate is, as Daniel Castro and Alan McQuinn of the Information Technology and Innovation Foundation observe, that “[i]nnovation is about risk, and if innovators fear they will be punished for every mistake . . . then they will be much less assertive in trying to develop the next new thing.”85 Meanwhile, the United States adopted a very different disposition that favored risk-taking and tolerated business failures and cultural disruptions. Disruptive technologies were embraced (or at least permitted) in the United States, resulting in the explosive growth of the Internet and America’s information technology sectors (computing, software, Internet services, etc.) over the past two decades. Those sectors have ushered in a generation of innovations and innovators that are now household names across the world, including in Europe.

The result of the general freedom to experiment in this arena was not only an outpouring of innovation that was unprecedented in recent times but also a boost for US competitive advantage overall.86 For example, a recent Booz & Company report on the world’s most innovative companies revealed that nine of the top 10 are based in the United States and that most of them are involved in computing.87 Another recent survey revealed that the world’s 15 most valuable Internet companies (based on market capitalizations) have a combined market value of nearly $2.5 trillion, but none of them are European while 11 of them are US firms.88 Meanwhile, the information technology market on either side of the Atlantic illustrates how investor money overwhelmingly flocks to US shores. The market capitalizations for America’s major tech companies overwhelm European tech firms.89

The data on the overall size of the respective tech markets on either side of the Atlantic provide an even more dramatic contrast. As of 2015, the market value of Apple, Google, and Facebook each exceeded the entire value of the European market for tech “unicorns,” or firms with a market value of over $1 billion. Airbnb’s market value alone exceeds the value of all of Germany’s billion-dollar technology companies combined.

Many European officials and business leaders are waking up to this grim reality and are wondering how to reverse this situation. Danish economist Jacob Kirkegaard of the Peterson Institute for International Economics notes that Europeans “all want a Silicon Valley. . . . But none of them can match the scale and focus on the new and truly innovative technologies you have in the United States. Europe and the rest of the world are playing catch-up, to the great frustration of policy makers there.”90

Unsurprisingly, European officials are unhappy that American innovators enjoy competitive advantages in many digital sectors. As a result, some European policymakers are increasingly looking to force their more restrictive policies on US-based digital innovators. 91 The easier way to “level the playing field” between digital rivals on either side of the Atlantic would be for Europe to relax its restrictive, risk-averse policies, to give their innovators a better chance of learning from marketplace experimentation.92 Of course, that would mean that European policymakers would need to be willing to embrace the possibility that many of those firms would fail, or to the extent they succeeded, that restrictive data collection policies and other regulations might need to be reformed.

Thus far, European officials have shown little willingness to embrace that option and are instead stepping up their efforts to regulate technology companies, especially US-based firms.93 In fact, within the so-called sharing economy, European governments have moved aggressively to limit or shut down ride-sharing provider Uber.94 Following a major strike by French taxi drivers during summer 2015, France went so far as to arrest two Uber executives.95 (Ironically, downloads of Uber’s mobile app increased following the arrests.96) There’s even talk in Europe of creating an EU-wide super-regulator, mostly to address concerns about US-based tech companies.97

Such moves are motivated by a fear of disruption and change.

Whether it is economic or social norms, failure is often not an option in some European countries; public policies will protect industries, organizations, professions, or even just cultural norms that are threatened by technological change. The irony, however, is that the more aggressively European officials seek to avoid the possibility of various short-term failures, the more prone the continent is to potentially far more dangerous and systemic failures in the long term.98 “The trouble with Europe’s broad attack on U.S. tech companies is that it hurts Europe above all,” observes Mike Elgan of eWeek. “Europe will never be able to regulate its way to tech competitiveness. It has to come from industry, not government.” Elgan correctly argues that Europe’s problems with America’s tech innovators “should be solved by European startups, innovation, [and] entrepreneurship not meddling EU commissions, politicians and judges.”99

Whether European officials are willing to take steps to reverse this predicament remains to be seen. Regardless, the lesson for US policymakers should be clear: if they want to continue to produce world-leading technology innovators, they must avoid Europe’s overly precautionary and highly risk-averse approach to policy. Permissionless innovation remains the better default policy position toward new entrepreneurs and technologies, no matter how disruptive they may be in the short term.

E. GLOBAL INNOVATION ARBITRAGE

As the preceding discussion indicates, when and where public policies or political attitudes are stacked against entrepreneurial opportunities, then innovation will be disincentivized and innovators will look to do business elsewhere. Thus, there’s an even more practical reason why policymakers should take seriously the importance of permissionless innovation as a policy disposition: we increasingly live in a world where “global innovation arbitrage” 100 or “regulatory arbitrage for permissionless innovation” is a reality.101 Just as capital now fluidly moves around the globe seeking out more hospitable regulatory treatment, the same is increasingly true for innovations. Innovators can, and increasingly will, move to those countries and continents that provide a legal and regulatory environment more hospitable to entrepreneurial activity.102

As noted, the United States essentially won the first round of the “Web Wars” and took a commanding lead in the battle for global digital supremacy in terms of Internet-enabled innovation. Again, this occurred because the United States got policy right. Unfortunately, America’s digital technology supremacy may be reversing itself with some new technological innovations. “As I watch our government go slow in promulgating rules holding back American innovation,” noted Sen. Cory Booker (D-NJ) at a US Senate Commerce Committee hearing in early 2015, we are “seeing technology exported from America and going other places.”103

Consider what’s been happening in such diverse fields as commercial drones, driverless cars, genetic testing, and the sharing economy as the global competition to attract innovation and investment on these fronts intensifies. In particular, consider how the United Kingdom has been taking steps on these fronts to attract innovators who are being shunned by US policymakers:

* Drones: US-based tech innovators such as Amazon and Google had been threatening to move their drone research offshore before the Federal Aviation Administration (FAA) finally started taking steps to liberalize its rules and open the skies for aerial innovation.104 Amazon even sent the FAA a letter warning stating, “Without the ability to test outdoors in the United States soon, we will have no choice but to divert even more of our [drone] research and development resources abroad.”105 Meanwhile, other countries have been opening their skies to drone innovation.106 Both the United Kingdom and Australia have been more welcoming to drone innovators.107
* Driverless cars: The United Kingdom is opening its doors— or roads, as the case may be—to autonomous vehicles, or “driverless car” technology.108 The New York Times noted recently that “the country is positioning itself as a giant test track for global automakers,” and that “[a] recent review of Britain’s transport laws provided a green light for testing driverless cars on public roads—something often not allowed on the streets of other European countries. The country’s policy makers also are completing industry guidelines to sidestep other potential roadblocks, like liability and insurance issues, that could still hamper carmakers’ plans for autonomous cars.”109
* Genetic testing: One of the more vivid recent examples of‑global innovation arbitrage involves 23andMe, which‑sells mail-order DNA-testing kits to allow people to learn more about their genetic history and their potential predisposition to various diseases.‑Unfortunately, the FDA is actively thwarting innovation on this front after ordering the company to halt sales in the United States.110 The agency has recently taken steps to loosen regulation of 23andMe, although only for narrowly defined purposes.111 On the other side of the Atlantic, UK officials seem to be welcoming the firm with open arms as the UK’s Medicines and Healthcare Products Regulatory Agency said the company’s test can be used there, albeit with caution.112
* Sharing economy: Sharing economy innovators are potentially at risk in the United States because of incessant bureaucratic meddling at the state and especially the local level.113‑If policymakers don’t take steps to liberalize the layers of red tape that encumber new sharing economy start-ups, it is possible that some of these companies will start to look for opportunities offshore. The United Kingdom’s Department for Business, Innovation & Skills recently published a white paper titled “Unlocking the Sharing Economy,” which discusses how the British government intends to embrace the many innovations that could flow from this space.114 The preface to the report opens with a telling passage from Matthew Hancock, a member of the UK Parliament and the Minister of State for Business, Enterprise, and Energy, in which he notes, “The UK is embracing new, disruptive business models and challenger businesses that increase competition and offer new products and experiences for consumers. Where other countries and cities are closing down consumer choice, and limiting people’s freedom to make better use of their possessions, we are embracing it.”115

That last line from Minister Hancock makes it clear that if other countries, including the United States, fail to create a more hospitable environment for innovation, then the United Kingdom and other countries will be all too happy to invite those companies to come set up operations there. The offshoring option is just as real in countless other sectors of the modern tech economy. Similar opportunities for such “global innovation arbitrage” exist for the Internet of Things and wearable tech, robotics, Bitcoin, and other advanced technologies. Moreover, this sort of jurisdictional competition for innovation can happen at multiple levels of government— cities, counties, states, countries, and continents.116

This reiterates why policy incentives matter so much. “America right now is the net exporter of technology and innovation in the globe, and we can’t lose that advantage,” notes Senator Booker. “[W]e should continue to be the global innovators on these areas.”117 But that will happen only if American policymakers are willing to embrace permissionless innovation for these new technologies.

INNOVATION OPPORTUNITY: Private Drones

Unmanned aircraft systems (UASs), or drones, are poised to become far more ubiquitous in coming decades.118 Many hobbyists already use drones for a remarkable range of applications. As New York Times tech columnist Farhad Manjoo has noted, drone enthusiasts “see almost limitless potential for flying robots” and they see drones as “a platform—a new class of generalpurpose computer, as important as the PC or the smartphone, that may be put to use in a wide variety of ways.”119 Drones could also have many important news-gathering uses for both professional media organizations and average citizens.120

The commercial benefits could also be profound. As Sen. Cory Booker (D-NJ) has argued, “[T]he potential possibilities for drone technology to alleviate burdens on our infrastructure, to empower commerce, innovation, jobs . . . to really open up unlimited opportunities in this country is pretty incredible to me.”121 A 2013 study from the Association for Unmanned Vehicle Systems International, which represents the industry, predicted $82.1 billion in economic impact between 2015 and 2025 from the integration of UASs into the nation’s airspace.122

Drones are already positively transforming many sectors, including agricultural and weather monitoring, disaster response management, law enforcement (especially missing persons searches), and entertainment services (such as movie production). Major tech innovators, such as Google,123 Amazon,124 and Facebook,125 are already actively experimenting with drone technologies to provide services to the public, but many smaller drone innovators exist (such as DJI, Parrot, and 3D Robotics). These manufacturers of commercial drones had revenue exceeding $600 million in 2014.126

Those numbers would likely be much larger if not for endless foot-dragging by federal regulators. Congress ordered the FAA to come up with a plan to integrate drones into domestic airspace by September 2015, but the agency missed the deadline and has continued to delay progress.127 This is partially due to the fact that private drones have already raised many safety and privacy concerns.128 The FAA invited comments in a proceeding about drone privacy,129 and legislation limiting private or commercial drone use has already been introduced at the federal level130 and in many states.131 In early 2015, the White House issued a memorandum addressing such concerns and creating a multistakeholder process to develop best practices for drone privacy.132

Some drone regulation is likely inevitable, but preemptive controls could curtail many of the benefits that could flow from relatively unrestrictive experimentation with UASs.133 Restrictions on news-gathering uses of private drones could also raise serious First Amendment concerns.134

It may be the case that existing laws and policies—property rights, nuisance laws, torts, “Peeping Tom” laws, etc.—could cover the most concerning privacy- infringing scenarios.135 For safety issues, UAS operators could simply be held liable in court for damages that they cause, much as automobile drivers can be held liable for their damages. New legal standards for UAS-related controversies will evolve gradually through a body of common-law cases, as they have for many other technologies.136

Generally speaking, however, permissionless innovation should guide policy decisions for the nation’s airspace.137 New rules must leave ample space for future innovation opportunities so that, like the Internet, airspace can become a platform for commercial and social innovation.138 Unfortunately, some companies have been exporting development of these technologies abroad owing to the uncertainty of the regulatory environment here in the United States.139

CHAPTER IV

HOW WE ADAPT TO TECHNOLOGICAL CHANGE

In this chapter, we consider why the worst fears about new technologies usually do not come to pass. The reason is simple: humans have the uncanny ability to adapt to changes in their environment, bounce back from adversity, and learn to become wiser and more resilient over time.

This has important ramifications for the policy debate between the precautionary principle mindset and the notion of permissionless innovation. If adaptation is not just possible but even extremely likely, then there is even less reason to preemptively restrict social and economic experimentation with new technologies and technological processes.

A. FROM PANIC TO EVENTUAL ADAPTATION

As chapter III noted, when new inventions first come on the scene, the initial reaction from philosophers, scientists, and pundits is often fear and loathing about the potential ramifications of technological change for both the culture and the economy. “Armageddon has a long and distinguished history,” Garreau notes. “Theories of progress are mirrored by theories of collapse.”1

In his magisterial history of apocalyptic theories, The Idea of Decline in Western History, Arthur Herman documented how such “declinist” thinking—or what Garreau referred to as “hell” scenarios—have been a pervasive, reoccurring feature of most past academic writing and social commentary. The irony of much of this pessimistic declinist thinking, however, is that, “[i]n effect, the very things modern society does best—providing increasing economic affluence, equality of opportunity, and social and geographic mobility—are systematically deprecated and vilified by its direct beneficiaries,” Herman says. “None of this is new or even remarkable.”2

Indeed, despite the fact that the general real-world trend has been in the direction of steady improvements in human health, welfare, and convenience, the skeptics persist in thinking that impending doom lies just around the corner. Even if the sky didn’t fall before as predicted, critics will always insist that this time it’s different! And many people believe them.

Chapter II offered some explanations for this strange phenomenon. In a nutshell, this behavior is rooted in our innate tendency to be pessimistic as well as a desire for greater certainty about what the future holds.3 By taking advantage of these tendencies, “the gloom-mongers have it easy,” notes Dan Gardner in his book, Future Babble: Why Expert Predictions Are Next to Worthless, and You Can Do Better, because their predictions “feel right to us. And that conclusion is bolstered by our attraction to certainty.”4

But just because those pessimistic predictions feel right, it doesn’t mean they are right. Again, the historical record is unambiguous: ongoing technological innovation has done more to improve the human condition that any other factor.

Yet, not only do the techno-critics consistently fail to appreciate what the historical record has to say about innovation fueling progress and prosperity, those critics also pay little attention to just how effectively humans adapt to ongoing technological change. “The good news is that end-of-the-world predictions have been around for a very long time, and none of them has yet borne fruit,” Garreau reminds us.5 Why not? Let’s return to his framework for the answer. After discussing the “Heaven” (optimistic) and “Hell” (skeptical or pessimistic) scenarios cast about by countless tech writers throughout history, Garreau outlines a third, and more pragmatic, “Prevail” option, which views history “as a remarkably effective paean to the power of humans to muddle through extraordinary circumstances.”6

The “Prevail” or “muddling through” scenario offers the best explanation for how we learn to cope with technological disruption and prosper in the process. As Garreau explains it, under the Prevail scenario, “humans shape and adapt [technology] in entirely new directions.”7 He rightly notes, “Just because the problems are increasing doesn’t mean solutions might not also be increasing to match them.”8 As John Seely Brown and Paul Duguid noted in their 2001 essay responding to “doom-and-gloom technofuturists”:

[T]echnological and social systems shape each other. The same is true on a larger scale. . . . Technology and society are constantly forming and reforming new dynamic equilibriums with far-reaching implications. The challenge . . . is to see beyond the hype and past the oversimplifications to the full import of these new sociotechnical formations.9

It is this process of “constantly forming and reforming new dynamic equilibriums” that is typically overlooked by technology critics. Or, to the extent the critics are willing to engage in a discussion on this matter at all, they often change the topic and instead stress the disruptions that happened along the way—i.e., the social or economic norms that were challenged by technological change.10

That technological change disrupts is, of course, a truism by its very nature.11 Something is lost in the process. In terms of economics, it may be a job or a business that is lost, or perhaps even an entire profession or sector that disappears. It terms of culture, it may be a particular art form or medium of expression. And in terms of society more generally, technological change might fundamentally alter the ways we interact with each other and the world around us.

All this is undoubtedly true, but what of it? What can we learn from this? What were the mechanics of that adaptive process? As social norms, personal habits, and human relationships were disrupted, what helped us muddle through and find a way of coping with new technologies? Likewise, as existing markets and business models were disrupted, how were new ones formulated in response to the given technological disruption? Finally, how did legal norms and institutions adjust to those same changes?

Individual and societal acclimation to technological change is worthy of serious investigation if for no other reason than it has continuously happened! And what is most remarkable about this process is that we humans have again and again figured out how to assimilate new technologies into our lives despite how much those technologies disrupted our personal, social, economic, cultural, and legal norms.12 We prevailed and prospered.

#### That’ll incrementally fit AI into existing frameworks, solving downside risk, while letting regulatory expertise develop to avoid stifling innovation

Dr. Ahmed Badran 21, Associate Professor of Public Policy at Department of International Affairs, College of Arts and Sciences, Qatar University, PhD in Public Policy from the University of Exeter, “Thoughts and Reflections on the Case of Qatar: Should Artificial Intelligence Be Regulated?”, in Artificial Intelligence in the Gulf Challenges and Opportunities, Ed. Azar and Haddad, p. 69-71

1 Introduction

Technological advances can be regarded as a double-edged weapon. On the one hand, many befits can be reaped from the utilization of new technologies to improve the quality of life for human beings in different areas. On the other hand, the recent technological developments, particularly in the area of computing and robotics, raised a fundamental question about the possibility of the newly developed AI innovations to act independently from human control and to make their own decisions, which may harm humanity. In this context, different scholars and technology experts have echoed their concerns about the potential threats that AI may pose in the absence of government oversight and regulations (Reed, 2018). From an economic point of view, many economists share the fear that AI applications and machines alongside the advances in computing and robotics may result in economic disruptions and higher rates of unemployment especially among low skilled workers (AI Forum of New Zealand, 2018). As such, AI applications are expected to result in job losses in all areas, including blue collars, white collars, and professional services (Russell & Norvig, 1994). At the same time, many activists and intellectuals are opposing the idea that governments should develop autonomous weapons and autonomous killing machines that work independently from human intervention and may select and destroy their own targets as this may result in significant security risks (Etzioni & Etzioni, 2017).

The ubiquity of AI in modern societies means that people, as well as governments, will be muddling through its legal and ethical ramifications for quite some time. The fast increase in AI applications raises fundamental questions about the potential impact of machines on the everyday lives of humans. As put by Scherer, ‘with each passing month, AI gains footholds in new industries and becomes more enmeshed in our day-to-day lives, and that trend seems likely to continue for the foreseeable future’ (Scherer, 2016). In this context, a valid inquiry would be whether AI applications will result in a better life and more efficient use of available resources, or they will pose threats, which might end humankind (Kohli, 2015). In general, AI cannot be seen as all good or all bad. It is a reality, it affects our lives in different shapes and forms, it provides opportunities, and it poses threats (Erdelyi & Goldsmith, 2018). The question now becomes, how could we deal with the AI threats in order to maximize the benefits and mitigate or minimize the risks? Addressing all the risks associated with AI goes beyond the scope of this chapter. Therefore, the chapter will focus on one aspect that is the policy and legal vacuum created by the AI revolution.

There are calls from scholars, AI practitioners, and technology leaders for a form of government regulation on AI activities and research in order to protect the public interest are gaining more attention. The founder of Tesler, Elon Musk, for instance, has regarded AI as being even more dangerous than nuclear weapons. In this regard, he wrote on Twitter, ‘I’m increasingly inclined to think there should be some regulatory oversight [of AI], maybe at the national and international level’. In the same vein, regulatory and legal scholars, including Matthew Scherer, have called for the development of an overall legal and regulatory framework, which guarantees the safety of AI innovations through government intervention. The idea of developing policies and guidelines to regulate AI programs is not an alien even for the AI communities and industries. The Association for the Advancement of Acritical Intelligence has looked into this issue; however, the AI researchers have concluded that there is no need to develop such guidelines as the threats and risks associated with AI are not certain (Reed, 2018). Scherer has commented on the growing calls for regulating AI by stating that ‘fear of technological change and calls for the government to regulate new technologies are not new phenomena. What is striking about AI, however, is that leaders of the tech industry are voicing many of the concerns’ (Scherer, 2016).

Despite this growing agreement among several AI community members on the importance of government regulation and intervention, the question is still how much intervention is needed. In innovation and technology-driven sectors such as AI, too much government intervention and heavy-handed regulations might hamper the innovation and progress of these sectors (Finale & Kortz, 2017). Moreover, restrictive government regulations may result in less efficient AI systems, forced design choices, and suboptimal outcomes (Beishon, 2018). Hence, the regulation of AI will not be an easy task given the different meanings of AI in different areas and the risks the diverse forms of AI pose at different levels.

In this context, the chapter argues that recent developments in AI call for regulatory intervention from governments in order to strike a balance between potential benefits and the expected threats and risks. Nonetheless, any attempt to regulate AI is bound by the meaning we associate with this concept as AI means different things to different people and poses diverse types of risks in different policy domains. Moreover, the chapter emphasizes that we should not rush at present to restrictively regulate AI in ignorance. Instead, an incremental and gradual approach for regulating AI is needed wherein a distinction can be made between AI products and innovations that can be regulated within the existing legal and regulatory framework and those required new regulations. To follow up on this argument, the chapter will be divided into two main sections. Section one sets the stage for the discussion of AI regulation and the regulatory challenges posed by this novel construct. In this regard, AI and the other related concepts are discussed alongside the different positions taken on regulating AI from the leading AI entities. Section two is devoted to the discussion of a proposed regulatory framework to regulate AI in Qatar. The last chapter concludes with some policy recommendations on how to regulate AI without hampering innovation in such a promising and fast-growing sector.

### 2NC---Regulation Fails

#### 1. Skills deficit---regulators lack expertise to evaluate AI and apply the rule

Dr. Julia Black 19, Professor of Law and Strategic Director of Innovation at the London School of Economics, DPhil from Oxford University, and Andrew Murray, Professor of Law at the London School of Economics, LLB from Edinburgh University, “Regulating AI and Machine Learning: Setting the Regulatory Agenda”, European Journal of Law and Technology, Volume 10, Number 3, https://ejlt.org/index.php/ejlt/article/view/722/978

5. The Regulatory Action

It is too late for us to put AI and ML back into a box. It may be that in areas which are already heavily regulated, such as medical products and applications, then the use of AI or ML will require prior regulatory approvals. But even if they are caught in an existing regulatory net, there is little evidence that regulators have the necessary capacity properly to evaluate all the actual and potential uses of AI in their regulatory domains. Asymmetries of knowledge and skills are amplified in the highly technical area of AI. And we can see from current debates in multiple areas that existing regulatory systems simply do not capture the use of AI and ML, allowing them to operate on the edges of existing regulatory perimeters or escape them entirely. The current domination by corporate players means that AI is likely to be developed and marketed in a similar fashion to internet products and online services. There will be both a consumer market and a commercial market for products and services and in all likelihood they will be regulated, if at all, in piecemeal fashion. But as noted, AI is also being rapidly used by governments themselves to deliver welfare provision (education, healthcare) [67] and exercise core functions of government (policing, justice) and indeed in the function of regulation itself. [68] Furthermore, we know from the long histories of regulation in other areas that companies, government bodies, NGOs and others will seek to reassure governments and consumers that formal regulation is not required; that they can and will act ethically and adopt such devices as codes and ethics boards to demonstrate that commitment. However, we also know from history that a commitment to ethics is important, indeed essential, for effective regulation, but is rarely sufficient on its own in the absence of very specific conditions which rarely exist in a highly competitive market.

#### 2. Evasion---dedicated developers easily hide

Dr. Michael Guihot 17, Senior Lecturer at the Commercial and Property Law Research Centre at Queensland University Technology Faculty of Law, Dr. Anne F. Matthew, Lecturer at the Commercial and Property Law Research Centre, Queensland University of Technology Faculty of Law, and Nicolas P. Suzor, Associate Professor at the Queensland University of Technology Faculty of Law and Recipient of an Australian Research Council DECRA Fellowship, “Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence”, Vanderbilt Journal of Entertainment and Technology Law, 20 Vand. J. Ent. & Tech. L. 385, Volume 20, Issue 2, Winter 2017, Lexis

7. Limited Enforcement Mechanisms and Jurisdiction Shopping

Added to the complexities outlined above, the major players in the development of AI - such as Google, Facebook, Microsoft, and Apple - are some of the biggest, most complex, and powerful corporations the world has seen. 203 They own and control what Marx might have described as the means of production in this field - that is, the vast array of superpowerful computers and the phalanx of the world's best and brightest mathematicians and engineers required to churn the algorithms necessary to create AI. 204 The power disparity between these players and government regulators, who often struggle to secure sufficient resources to operate, highlights the difficulties that might be faced by a regulator in trying to regulate these companies. 205

The fact that the technology is relatively opaque 206 also makes it easier for firms to hide wrongdoing and evade regulation. Volkswagen, for example, was able to create specific code to identify the tests used by regulators to measure emissions and make its car engines appear to run more cleanly than when in normal use. 207 Similarly, recent reports suggest that Uber created a version of its app specifically designed to identify users likely to be regulators and prevent them from accessing the system to investigate concerns or collect evidence. 208

#### 3. Timing---it’s reactive, adopted only when already obsolete

Harriet Moynihan 21, Acting Director of the International Law Programme at Chatham House, MA with Honors from the Trinity Hall, University of Cambridge, and Marjorie Buchser, Executive Director of the Digital Society Initiative, MA in Comparative and International Studies from the Swiss Federal Institute of Technology in Zurich (ETHZ), MA in Political and Social Sciences from the Université of Lausanne, “Can Global Technology Governance Anticipate the Future?”, Chatham House Expert Comment, 4/27/2021, https://www.chathamhouse.org/2021/04/can-global-technology-governance-anticipate-future

Technology governance is beset by the challenges of how regulation can keep pace with rapid digital transformation, how governments can regulate in a context of deep knowledge asymmetry, and how policymakers can address the transnational nature of technology.

Keeping pace with, much less understanding, the implications of digital platforms and artificial intelligence for societies is increasingly challenging as technology becomes more sophisticated and yet more ubiquitous.

To overcome these obstacles, there is an urgent need to move towards a more anticipatory and inclusive model of technology governance. There are some signs of this in recent proposals by the European Union (EU) and the UK on the regulation of online harms.

Regulation failing to keep up

The speed of the digital revolution, further accelerated by the pandemic, has largely outstripped policymakers’ ability to provide appropriate frameworks to regulate and direct technology transformations.

Governments around the world face a ‘pacing problem’, a phenomenon described by Gary Marchant in 2011 as ‘the growing gap between the pace of science and technology and the lagging responsiveness of legal and ethical oversight that society relies on to govern emerging technologies’.

This ever-growing rift, Marchant argues, has been exacerbated by the increasing public appetite for and adoption of new technologies, as well as political inertia. As a result, legislation on emerging technologies risks being ineffective or out-of-date by the time it is implemented.

Effective regulation requires a thorough understanding of both the underlying technology design, processes and business model, and how current or new policy tools can be used to promote principles of good governance.

Artificial intelligence, for example, is penetrating all sectors of society and spanning multiple regulatory regimes without any regard for jurisdictional boundaries. As technology is increasingly developed and applied by the private sector rather than the state, officials often lack the technical expertise to adequately comprehend and act on emerging issues. This increases the risk of superficial regulation which fails to address the underlying structural causes of societal harms.

#### 4. Capture

Dr. Michael Guihot 17, Senior Lecturer at the Commercial and Property Law Research Centre at Queensland University Technology Faculty of Law, Dr. Anne F. Matthew, Lecturer at the Commercial and Property Law Research Centre, Queensland University of Technology Faculty of Law, and Nicolas P. Suzor, Associate Professor at the Queensland University of Technology Faculty of Law and Recipient of an Australian Research Council DECRA Fellowship, “Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence”, Vanderbilt Journal of Entertainment and Technology Law, 20 Vand. J. Ent. & Tech. L. 385, Volume 20, Issue 2, Winter 2017, Lexis

6. Agency Capture

Regulatory failure due to agency capture occurs where regulators become sympathetic towards the industry they are regulating. This can be the result of any number of factors, such as a high frequency of interaction between industry and regulators, industry representatives "buying off" regulators with gifts like free lunches or sponsorship to attend conferences, or a "revolving door" for employees between regulatory agencies and industry. 201 While each of these problems is relatively common throughout innovating industries, the AI industry is particularly susceptible to the revolving door issue. 202 The information asymmetry issue where AI companies hold all the relevant information about the technology makes the knowledge and expertise acquired by employees of AI developers particularly valuable to regulators, which are likely to be interested in employing former AI developers when (and if) they can.

### 1NC---Democracy Bad

#### Democratic peace is statistically disproven---it’s conflict driving

Dr. Daina Chiba 21, Associate Professor of Political Science in the Department of Government and Public Administration at the University of Macau, Ph.D. in Political Science from Rice University, LL.M in Jurisprudence and International Relations from Hitotsubashi University, and Dr. Erik Gartzke, Professor of Political Science at the University of California, San Diego, PhD in Political Science from the University of Iowa, “Make Two Democracies and Call Me in the Morning: Endogenous Regime Type and the Democratic Peace”, 2/19/2021, https://dainachiba.github.io/research/make2dem/Make2Dem.pdf

The democratic peace—the observation that democracies are less likely to fight each other than are other pairings of states—is one of the most widely acknowledged empirical regularities in international relations. Prominent scholars have even characterized the relationship as an empirical law (Levy 1988; Gleditsch 1992). The discovery of a special peace in liberal dyads stimulated enormous scholarly debate and led to, or reinforced, a number of policy initiatives by various governments and international organizations. Although a broad consensus has emerged among researchers regarding the empirical correlation between joint democracy and peace, disagreement remains as to its logical foundations. Numerous theories have been proposed to account for how democracy produces peace, if only dyadically (e.g., Russett 1993; Rummel 1996; Doyle 1997; Schultz 2001).

At the same time, peace appears likely to foster or maintain democracy (Thompson 1996; James, Solberg, andWolfson 1999). A vast swath of research in political science and economics proposes explanations for the origins of liberal government involving variables such as economic development (Lipset 1959; Burkhart and Lewis-Beck 1994; Przeworski et al. 2000; Acemoglu and Robinson 2006; Epstein et al. 2006) and inequality (Boix 2003), political interests (Downs 1957; Bueno de Mesquita et al. 2003), power hierarchies (Moore 1966; Lake 2009), third party inducements (Pevehouse 2005) or impositions (Peceny 1995; Meernik 1996), geography (Gleditsch 2002b), and natural resource endowments (Ross 2001), to list just a few examples. Each of these putative causes of democracy is also associated with various explanations for international conflict. Indeed, some as yet poorly defined set of canonical factors may contribute both to democracy and to peace, making it look as if the two variables are directly related, even if possibly they are not.

We seek to contribute to this literature, not by proposing yet another theory to explain how democracy vanquishes war, but by estimating the causal effect of joint democracy on the probability of militarized disputes using a quasi-experimental research design. We begin by noting that some of the common causes of democracy and peace may be unobservable, generating an endogenous relationship between the two. Theories of democracy and explanations for peace are at a formative state; it is not possible to utilize detailed, validated and widely accepted models of each of these processes to assess their interaction. Indeed, to a remarkable degree democracy and peace each remain poorly understood and weakly accounted for empirically, despite their central roles in international politics. We address the risk of spurious correlation by applying an instrumental variables approach. Having taken into account possible endogeneity between democracy and peace, we find that joint democracy does not have an independent pacifying effect on interstate conflict. Instead, our findings show that democratic countries are more likely to attack other democracies than are non-democracies. Our results call into question the large body of theory that has been proposed to account for the apparent pacifism of democratic dyads.

#### Democracy causes Nigerian state collapse and civil war

Dr. Moses E. Ochonu 19, Cornelius Vanderbilt Chair in History and Professor of African History at Vanderbilt University, PhD and MA in African History from the University of Michigan, BA in History from Bayero University, Graduate Certificate in Conflict Management from Liscomb University, “Why Liberal Democracy is a Threat to Nigeria’s Stability”, Logos: A Journal of Modern Society & Culture, May 2019, http://logosjournal.com/2019/liberal-democracy-is-a-threat-to-nigerias-stability/

In 2015, Nigeria, a country of about 190 million, spent $625 million to conduct federal and local elections. By comparison, India, with a population of 1.2 billion, spent $600 million on its 2015 election, according to figures released by the Electoral Commission of India (ECI).[1]

In 2019, the election budget of Nigeria’s Independent Electoral Commission (INEC) rose to $670 million. This represents about 2.5 percent of Nigeria’s $28.8 billion budget for 2019, a portion of which is being financed through borrowing. To put the electoral spending in context, more than half of the country subsists on about a dollar a day, and the country recently acquired the dubious distinction of being named the poverty capital of the world, with more people living in extreme poverty there than in any other country.[2] Key infrastructures and services such as roads, railway, electricity, water supply, healthcare, and education are severely inadequate, requiring urgent investments and interventions.

Election-related expenditure is expected to rise in the near future as INEC implements a wider slate of digital technologies to combat manipulation and improve the integrity of the electoral process. For comparison, Nigeria typically devotes about 7 percent of its budget to education. And yet Nigeria continues to maintain a four-year election cycle, with smaller by-elections occurring in between. This electoral calendar guarantees that about $1 billion is spent on elections every four years. As the electoral price tag has grown, democratic dividends have plummeted.

Nigeria’s predicament is a microcosm of the phenomenon of rising financial costs of elections in Africa and diminishing returns on democracy. Across the continent, the cost of electoral democracy is increasing and threatens the delivery of social goods. As African countries battle myriad socioeconomic challenges, the question needs to posed: is it wise for these countries to continue to spend a large percentage of their revenue every four or five years on a political ritual with fewer and fewer positive socioeconomic consequences for their populations? Is this expensive, periodic democratic ritual called election worth its price?

It is not only the monetary cost of elections that now threatens to defeat their purpose and engender disillusionment and, along with disillusionment, the erosion of trust in the state and its ability to produce and distribute public goods. The social cost of periodic elections has been arguably greater, depleting, with each election cycle, the residual stability of the state and the credibility of its institutions.

Elections conducted in Nigeria since the return of civilian rule in 1999 have brought with them anxiety, tension, death, violence, and dangerous rhetoric that, taken together, have frayed the national political and social fabric. Elections have widened fissures and intensified preexisting primordial cleavages.

I can recall no electoral cycle since at least 2003 that was not been accompanied by fears of Nigeria’s disintegration or at the very least the acceleration of its demise. In 2007 and 2011, post-election violence claimed hundreds of lives in Northern Nigeria as supporters of then candidate Muhammadu Buhari rioted after his loss. In the 2019 presidential and national assembly elections, at least 46 people were reported to have died from election-related violence. In the state assembly and governorship elections two weeks later on March 9, 2019, another 10 people died across five states in what the Sunday Tribune newspaper described in its headline as “another bloody election.”[3]

Two riders below the same Sunday Tribune headline encapsulate the turbulent character of Nigerian elections. One was “Thugs, vote buyers, arsonists take over on election day”; the other was “Nigerians condemn militarization of elections in Rivers, Bayelsa, Kwara, Akwa Ibom, Benue,” a reference to the government’s deployment of soldiers and other military assets to opposition strongholds before and during the election. The involvement of soldiers and other military personnel in the election was a brazen violation of Nigeria’s Electoral Act, an action which many observers interpreted as the incumbent administration’s effort to use its might to manipulate the election in states held by the opposition.

Every election cycle in Nigeria sees massive, fear-induced demographic mobility as members of different ethnic groups and religions relocate to areas considered dominated by their kinsmen and co-religionists to await the conclusion of elections that often degenerate into communal clashes especially in the volatile north of the country.

Periodic national elections have thus worsened Nigeria’s notoriously frail union and caused apathy and discontent. The Nigerian people, the major stakeholders in Nigeria’s democracy, have grown weary of being periodically endangered and rendered pawns in an elaborate elite ritual with little or no consequence for their lives.

Electoral aftermaths have not improved economic conditions or strengthened the capacity of citizens to hold elected leaders accountable. Moreover, as I shall discuss shortly, the familiar abstract freedoms that democracy, lubricated by periodic elections, can confer on citizens who participate in such exercises, have eluded Nigerians.

The result has been noticeable apathy represented most poignantly by voter turnout, which declined from a peak of 69.1 percent in 2003 to 46.3 percent in 2015 and to about 35 percent in 2019. In the same 2019 election cycle, turnout declined to less than 20 percent in the governorship and state assembly elections, with many Nigerians on social media stating that they had lost faith in the electoral process and that the official results of the presidential elections two weeks earlier had shown that their votes would not count towards the declared outcome.

Voter apathy alone is not an indication of democratic disillusionment but it can portend or indicate something more devastating: diminishing trust in the state, its institutions, and its processes.

Such a trust deficit exists already and it predated the return of civilian rule in 1999 after about two decades of military dictatorship. However, by all theoretical formulations, such a cumulative loss of confidence in the transactional sociopolitical contract between the state and citizens should be corrected by the democratic ideals of voting, representation, and accountability. This has not happened in Nigeria. In fact, the opposite scenario is visible: a negative correlation between successive electoral cycles and citizens’ trust in the Nigerian state. Therein lay the paradoxical consequences of democratic practice in Nigeria.

If elections are increasingly burdensome as they have become in Nigeria, the corrective potential of democracy, broadly speaking, is lost. Citizens consequently lose faith in the state and resort to self-help, including criminal self-help. That is how states collapse. Nigeria is not far off this possibility.

In Nigeria, recent political realities reveal a blind spot of pro-democracy advocacy: without the modulating effect of decentralization, sustained economic growth, a growing, secure middle class, and a literate, hopeful poor, liberal democracy can do and has done more damage than good. Liberal democracy has ironically become both an incubator and protector of mediocrity, corruption, and bad governance. The overarching casualty has been Nigeria’s very stability.

#### Nigerian instability escalates to global great power war

Charles A. Ray 21, Member of the Board of Trustees and Chair of the Africa Program at the Foreign Policy Research Institute, Former U.S. Ambassador to the Kingdom of Cambodia and the Republic of Zimbabwe, “Does Africa Matter to the United States?”, Foreign Policy Research Institute, 1/11/2021, https://www.fpri.org/article/2021/01/does-africa-matter-to-the-united-states/

Africa matters in terms of size, population, and rate of population growth. It is the continent currently most affected by climate change but is also a continent that can have a devastating impact on climate change globally because of the importance of the Congo Basin rainforest, which is the second-largest absorber of heat after the Amazon rainforest. The destruction of this important ecosystem could further accelerate global warming. As residents of the region come into increasing contact with the animals of the rainforest, this region could be the origin of the world’s next viral pandemic. Violent extremism and terrorism are increasing in Africa, and while now mostly localized, the danger has the potential to spread beyond the continent. Crises—natural and man-made—cause massive relocations of populations, both on the continent and abroad, which can have negative economic, social, and political impacts.

Why Africa Matters

The African continent is the world’s second-largest, with the second-fastest growth rate after Asia. With 54 sovereign countries, four territories, and two de facto independent states with little international recognition, the continent has a current population of 1.3 billion. By 2050, the continent’s population is predicted to rise to 2.4 billion. By 2100, Nigeria, Africa’s most populous country, will have a population of one billion, and half the world’s population growth will be in Africa by then.

The population of African countries is also overwhelmingly young. Approximately 40% of Africans are under 15, and, in some countries, over 50% is under 25. By 2050, two of every five children born in the world will be in Africa, and the continent’s population is expected to triple. These developments have positive and negative potential impacts on the United States and the rest of the world. Young Africans have, for the most part, completely skipped the analog age and gone directly digital. Comfortable with technology, they form a huge potential consumer and labor market. If, on the other hand, the countries of Africa fail to develop economically and do not create gainful employment for this young population, then there is the risk that they will become a huge potential source of recruits to extremist and terrorist movements, which currently target disadvantaged and disenchanted youth.

Lack of economic opportunity, increased urbanization, and climate-fueled disasters will also contribute to movement of people seeking better lives, which will impact economies and security not only on the continent of Africa, but also the economic and security situations around the world. Nations, lacking adequate critical infrastructure, education, and job opportunities are ripe for internal unrest and radicalization. In particular, inadequate health delivery systems, when coupled with natural disasters, such as droughts or floods that limit food production, cause famine and mass movements of populations.

The Challenges for U.S. Policy

Prior to World War II, the U.S. policy towards Africa was not as active as it was toward Europe, Asia, or Latin America. During the Cold War, Africa policy was primarily viewed from a perspective of super-power competition. The end of the Cold War and the rise of international terrorism introduced this as a major component in U.S. Africa policy along with competition with a rising China and increased Chinese engagement in Africa.

Before his first official trip to Kenya, U.S. President Barack Obama said, “Africa had become an idea more than an actual place . . . with the benefit of distance, we engaged Africa in a selective embrace.” This is probably an apt description of U.S. policy towards African nations despite the bipartisan nature of that policy. The United States, with the many domestic and international issues it has to cope with, can ill afford to continue to ignore Africa. Going forward, U.S. policy must include a hard-headed look at where Africa fits in policy priorities.

The incoming Biden administration will face a number of important issues and challenges as it develops its Africa policy. The most pressing issues are the following:

Climate Change: Climate change is an existential problem that affects the entire globe, but Africa has probably suffered more from the effects of climate change than other continents—and the problem will only get worse with time. In an October 2020 article, World Meteorological Organization (WMO) Secretary-General Petteri Taalas said,

Climate change is having a growing impact on the African continent, hitting the most vulnerable hardest, and contributing to food insecurity, population displacement and stress on water resources. In recent months we have seen devastating floods, an invasion of desert locusts and now face the looming specter of drought because of a La Nina event. The human and economic toll has been aggravated by the COVID-19 pandemic.

Climate change impacts water quality and availability, and millions in Africa will likely face persistent increased water stress due to these impacts. A multi-year drought in parts of South Africa, for instance, threatened total water failure in several small towns and had livestock farmers facing financial ruin. Another pressing climate-change issue is the need for protection of the Congo Basin rainforest. This 178-million-hectare rainforest is the world’s second largest after the Amazon and is currently threatened by agricultural activities in Cameroon, Central African Republic, Democratic Republic of Congo, Republic of the Congo, Equatorial Guinea, and Gabon. Countries in the Congo Basin need to address the preservation issue, while also enabling sustainable agricultural activities to ensure food security for the region’s population. In addition to the impact on global climate caused by destruction of the rainforest, such destruction also brings human populations into closer contact with the region’s animals, creating the risk of future animal-to-human transmission of new and possibly more virulent viruses similar to COVID-19, which will have a global impact. In a January 2021 CNN report, Dr. Jean-Jacques Muyembe Tamfum, who as a researcher helped discover the Ebola virus in 1976, warned of possible new pathogens that could be as infectious as COVID-19 and as virulent as Ebola.

Rule of Law/Mitigation of Corruption: A key to African development, given the increasing urbanization, population increases, and youthfulness of the continent’s population, will be an increase in domestic and international investment to build the industries that can provide meaningful employment and improved standards of living. In order for this to be successful, African nations will need to address the issues of rule of law and corruption. Investors will not risk money if the business climate comes with a level of political risk that is too high. Government leaders throughout Africa need to establish legislation that provides an acceptable level of security for investments and take action to curb the endemic corruption that currently discourages investment. Corruption in Africa ranges from wholesale political corruption on the scale of General Sani Abachi’s looting of $3-5 billion of state money during his five years as Nigeria’s military ruler to the bribes paid by businessmen to police and customs officials. The “tradition” of having to pay bribes, or “sweeteners,” drives away domestic investment and scares away foreign investment, leaving many countries mired in poverty.

Violent Extremism and Terrorism: A number of African nations are currently plagued with rising extremist movements. While primarily a domestic issue, the mass movement of people fleeing violence and the disruption of economic activity have the potential to negatively impact the rest of the world. African nations need regional responses to curb extremist and terrorist organizations, many of which are supported by international terrorist organizations, such as ISIS and al Qaeda. In addition, the underlying conditions that helped to create these movements must be addressed. Terrorist groups in Africa range from relatively large and dangerous groups, such as Boko Haram, a group in Nigeria that has received support from al Qaeda and that aims to implement sharia law in the country; Al-Shabab, an al Qaeda affiliate aiming to overthrow the government in Somalia and to punish neighboring countries for their support of the Somali regime; and Uganda’s Lord’s Resistance Army, a fundamentalist Christian group. Terrorist groups in the fragile political climate of Libya also pose a threat to sub-Saharan Africa.

Great Power Competition: As the world’s second-largest economy, and with its increasing participation in international activities, China will continue to be a factor in Africa for the foreseeable future. This, however, is more a problem for the nations of Africa than it is for the rest of the world. The West can compete best by outperforming China in areas of strength by providing those goods and services that are unquestionably superior, and let African governments decide how to deal with China and its often-predatory lending practices and the Chinese tendency to import Chinese workers for its projects and investments rather than hiring locals. At the same time, Russia, which did not completely turn away from Africa at the end of the Cold War as many in the West sometimes believe, must still be considered a significant factor on the African landscape. In an effort to compensate for Western sanctions and to counter U.S. and Western influence, Russia is once again increasing its presence on the continent. Russian mercenaries, in exchange for diamond mining rights, have trained military forces in the Central African Republic, raising concerns about human rights abuses. Of particular concern is the presence of the Wagner Group, a private military company associated with Yevgeny Progozhin, a Russian oligarch with close ties to Vladimir Putin, who was indicted in the United States for trying to disrupt the 2016 U.S. elections. To date, Russia has, in addition to seeking basing rights, signed military cooperation agreements with 28 African nations. Russian activity is a combination of military and commercial, with Progozhin at the center of both. From 2010 to 2018, Russia nearly tripled its trade with African countries. While the activities of both Russia and China in Africa are of concern, and should be closely monitored, neither is of critical importance to U.S. national security.

With climate change, disease outbreaks, famine, extremism, and inter-ethnic violence, Africa will still experience crises in the foreseeable future that will be beyond the capacity of most nations on the continent to deal with. Climate change is probably the greatest cause of humanitarian crises in Africa, but mainstream media outside the continent either fail to notice or under-report them. Some of the crises, like Ebola or the next viral infection, can impact the rest of the world. These crises will cause starvation, mass movement of people, and increase internal and regional instability. Africa matters to the United States and the rest of the world. Its impacts can be felt far beyond the continent’s borders, but if approached as a partner rather than as a patron—with a focus on assisting African nations to improve governance, build critical infrastructure, boost domestic economies, and provide essential services to all—then Africa can be a positive contributor on the global stage.

#### Democracy makes disease control impossible

Zhifa Zhou 21, Associate Professor at the Institute of African Studies at Zhejiang Normal University and Pan Qu, Postgraduate at the Institute of African Studies at Zhejiang Normal University, “The Root Cause of the Failure of American COVID-19 Governance Based on the Criticism of Liberal Democracy From Error-Tolerant Democracy”, Philosophy Study, Volume 11, Number 7, July 2021, https://www.davidpublisher.com/Public/uploads/Contribute/60ff9cfb4589c.pdf

Introduction

Whether liberal democracy contributed to the COVID-19 governance was a hot topic in 2020 (“Democracy and Rise of Authoritarianism in COVID-19 World”, 2020). At the end of January, 2020, when COVID-19 witnessed the lockdown of Wuhan City, the West generally agreed that China lacked freedom of speech and the inertia of a rigid bureaucratic structure, and the national censorship system kept the whistle blower Dr. Wenliang Li silent, which led to the disease out of control (Mérieau, 2020). Democracies’ confidence mainly came from Amartya Sen’s research on the famine. Sen (1999) has claimed that no substantial famine has ever occurred in any independent and democratic country with a relatively free press and there is no exception to this rule. Citizens in democracies can expect governments to be more candid, transparent, and responsible in dealing with all kinds of crises, which authoritarian countries usually cannot (Berengaut, 2020; Bollyky & Kickbusch, 2020). So Steve Bloomfield (2020) has regarded that if China had a free press and transparent government, the pandemic could be brought under control before the outbreak. In conclusion, freedom plus democracy equals the COVID-19 antidote according to Western standards, although Wilson and Wisongye have found that social media rumors can exploit the right to freedom of speech and erode people’s health benefits (New York Times, 2021; Bollyky & Kickbusch, 2020). However, since March, 2020, with Western democracies seriously affected by COVID-19, their superiority of the political system has begun to expose its untrue and fatal defects. Especially when Wuhan began to lift its blockade on April 8, 2020 (People.cn, 2020), scholars and journalists began to question whether democracies had the ability to deal with the crisis better than China (Mérieau, 2020). Liberal democracy in the United States has not proved that it is more conducive to the COVID-19 governance than authoritarianism since 2020. From a global perspective, not only do most democracies fail to contain the spread of COVID-19, but almost all of the 10 most affected countries are liberal democracies (Coronavirus Resource Center, 2021). Their policy responses have a poor effect in reducing the death toll in early stages of the crisis, as shown that democratic political institutions may be at a disadvantage in responding quickly to COVID-19 (Cepaluni, Dorsch, & Branyiczki, 2020). More surprising is that the COVID-19 pandemic is so serious in the United States, yet no government officials have been removed from office because of their inactivity in fighting against the corona-virus. People doubt whether American accountability mechanism is still working. However, two impeachments against President Trump indicate that it seems to function quite well (Valenta & Valenta, 2017; Herb, Raju, Fox, & Mattingly, 2021). The direct loss to the United States caused by Russiagate and incitement of insurrection is far less than the pain caused by the failure of the COVID-19 governance, but no any official in the United States is responsible for it. If it again faces infectious diseases similar to COVID-19, will it repeat this unprecedented tragedy? Can liberal democracy and the separation and balance of powers push American president to act more aggressively? Error-tolerantism explains that the fundamental reason for the failure of American COVID-19 governance is a serious misunderstanding of the concept of freedom (Zhou, 2018; 2019; Zhou, Tan, & Liu, 2020). Liberalism has witnessed a rare scene: In the context of COVID-19, the president, governors, magistrates, and the public (Emery, Schwebke, & Park, 2020; Sullum, 2020; Behrmann, 2020; Kenton, 2020; Strano, 2020) have severe misunderstanding of freedom that cost more than American 600,000 lives (Coronavirus Resource Center, 2021).

In response to the above phenomenon, error-tolerantism as the development of liberalism defines liberty from a new perspective and shows a stronger explanatory power than liberalism (Zhou et al., 2020). The right paradigm of error-tolerantism, the right to be wrong (right to trial and error) as an original right and mutual empowerment theory, instead of natural rights theory and social contract theory, divides liberty into the right to liberty in innovative fields, right to be wrong as an original right, and the right to be right in non-innovative fields as sub-rights. The lockdown of Wuhan means that Chinese government has excised the power to be wrong as an original power, but the West criticized it with the right to liberty at the level of sub-rights, which is the first error in understanding liberty during American COVID-19 governance; after Wuhan effectively controlled COVID-19, its governance has transformed from an innovative field to a non-innovative one. Then, liberties in non-innovative fields as the sub-rights level, such as wearing face masks, keeping social distancing, showing health codes, are formed definitely (Zhou et al., 2020). However, wearing masks has been regarded as a sign of political oppression rather than a simple hygienic measure by the United States (Kahanel, 2021). Since liberalism has a major misunderstanding of the concept of liberty, liberal democracy based on the philosophy of liberalism should be deeply reflected or even reconstructed, and it is very reasonable for error-tolerant democracy constructed based on error-tolerantism to explore the defects of liberal democracy in American COVID-19 governance. Therefore, we first review scholars’ relevant research on American democracy and the COVID-19 governance, and then based on the theory of error-tolerant democracy, discuss the defects of liberal democracy and American political system that are unable to cope with the crisis of the century.

#### Future pandemics are inevitable---extinction

Dr. Matt Boyd 21, Research Director at Adapt Research Ltd, PhD in Philosophy of Evolution & Cognition from the Victoria University of Wellington, BA from Massey University, and Nick Wilson, Research Professor in the Department of Public Health at the University of Otago, “Optimizing Island Refuges Against global Catastrophic and Existential Biological Threats: Priorities and Preparations”, Risk Analysis: An International Journal, Wiley Online Library

1 INTRODUCTION

Our world is vulnerable to global catastrophic risks (GCRs) or existential risks (Bostrom, 2019; Ord, 2020). GCRs are so disastrous because they affect one or more systems critical to humanity, and spread to affect the entire planet (Avin et al., 2018). Existential risks threaten to eliminate humanity or permanently curtail its potential (Ord, 2020). Some of these risks are natural, for example asteroid or comet impact, supervolcanic eruption, naturally occurring pandemic, or various cosmic events (Bostrom & Cirkovic, 2008; Ord, 2020). Many others are the result of human activities, for example nuclear war, anthropogenic climate change, nonaligned artificial intelligence, engineered biological threats, geoengineering, or inescapable totalitarianism (Bostrom & Cirkovic, 2008; Ord, 2020).

There are three phases to an existential catastrophe: origin, scale up, and reaching every last human (Cotton-Barratt, Daniel, & Sandberg, 2020). Following any near miss, there would be a period where recovery of humanity's long-term potential may or may not be realized (Baum et al., 2019). Failure to anticipate or mitigate these threats risks undesirable trajectories for human civilization (Baum et al., 2019).

In addition to the present generation's obvious self-interest in continuing to exist, the perspective of long-termism suggests that humanity ought to mitigate these risks due to the potential immense value of future human generations (Beckstead, 2013), a desire to see aspects of the human project continue across time and perhaps the universe (Bostrom, 2003; Scheffler, 2013), and the potential cosmic significance of preserving intelligent life on Earth (Ord, 2020). A number of philosophical defenses of long-termism have been published (Beckstead, 2013; Greaves & MacAskill, 2019). Importantly, these long-term outcomes are largely under human control because most of the risk is probably anthropogenic (Beard & Torres, 2020; Ord, 2020).

1.1 Mitigating Existential Threats

It is too simplistic to think of existential risks as mere causes that are followed by a sequence of effects. We should think of risks as the product of hazards, vulnerabilities, and exposures (Liu, Lauta, & Maas, 2018). Hazards are the precipitating cause of a catastrophe, vulnerabilities are the inability of critical systems to withstand hazards, and exposures are the features of human society that turn this system damage into harm to populations (Beard & Torres, 2020). Mitigation of existential threats involves preventing their emergence, responding if the threat spreads, and building resilience so the threat does not lead to the death of every last human or leave humanity with permanently curtailed prospects (Cotton-Barratt et al., 2020). After a threat has passed, there may also be a series of limiters that might prevent the reemergence of a flourishing humanity (Baum et al., 2019). One such limiting factor could be the loss of technological society and know-how.

In order to achieve immunity from existential threat, humanity will need a period where it preserves its potential and protects itself from risks (Ord, 2020). Various methods have been proposed to address vulnerabilities and hence shift the probability of existential risk. These suggestions include: improved international focus, governance, and cooperation such as through the United Nations (Boyd & Wilson, 2020), imitating existing frameworks such as the Sendai framework for disaster risk reduction (Avin et al., 2018), achieving the United Nations Sustainable Development Goals (Cernev & Fenner, 2020), or extreme surveillance for threats (Bostrom, 2019). Toby Ord lists 38 specific measures across eight existential threats, and an additional 12 avenues to explore that address risks in general terms (Ord, 2020).

1.2 Biological Threats

Pandemic viruses with high case fatality could potentially infect a majority of the population. Deliberate biological events (DBEs) have occurred before (Millet & Snyder-Beattie, 2017a), will likely occur again, and could pose a threat to humans as great as nuclear war (Kosal, 2020). New technologies such as artificial intelligence could amplify biothreats in a number of ways (O'Brien & Nelson, 2020). These risks are increased because the Biological Weapons Convention (BWC) has no verification system (Dando, 2016), and has been violated in the past (Gronvall, 2018). It would only take one unanticipated or accidental event for a bioweapon (or laboratory accident) to become a catastrophic threat. The U.S. National Academies of Sciences specifically warns against synthetic biology and xenobiology (Gomez-Tatay & Hernandez-Andreu, 2019) and it is argued that a state-sponsored bioweapon attack is the greatest current threat (Sandberg & Nelson, 2020). See the Supporting Information for further details on biological threats. Global preparedness through the One Health approach, global health security projects, and the need to integrate health and the GCR field (Millet & Snyder-Beattie, 2017b) are important. But as the COVID-19 pandemic has shown, there may be important overlooked aspects or misunderstood risks that could make any suite of general preparation inadequate. Therefore, last lines of defense may be required, such as refuges.

#### Existential warming is inevitable AND causes a collapse into extreme authoritarianism---only transitioning from democracy solves

Dr. Chien-Yi Lu 21, PhD and MA in Government from the University of Texas, Austin, Visiting Scholar at Harvard University, Associate Research Fellow at the Institute of European and American Studies of Academia Sinica, Surviving Democracy: Mitigating Climate Change in a Neoliberalized World, Paperback Edition, 12/13/2021, p. 1-2

The fact that the scientific knowledge on the human contribution to climate change entered human society through the most advanced democratic societies should have been a cause for celebration. Given the congruence of climate mitigation and public interests, the problem of climate change should have been considered solved decades ago. Several decades of inaction later, however, arguments are proliferating that democracy is exactly the reason for inaction.

In The Collapse of Western Civilization, historians Naomi Oreskes and Erik Conway travel to the future to look back and offer a forensic analysis on the climate-induced Great Collapse of Western Civilization of 2074 (2014: 63). The future historians’ forensic report states that “[a]s the devastating effects of the Great Collapse began to appear, the nation-states with democratic governments… were at first unwilling and then unable” to deal with the crisis. These democratic governments realized that they had no “infrastructure and organizational ability to quarantine and relocate people” as “food shortages and disease outbreaks spread and sea level[s] rose.” In China, where there was centralized government, the crisis was handled much more adequately, leading to survival rates exceeding 80%, a development that “vindicated the necessity of centralized government” (2014: 51–2). The gist of The Collapse of Western Civilization is not about critiquing democracy per se but a warning against the stubborn inaction mandated by market fundamentalism that has hijacked Western democracies.1 In their previous book, Merchants of Doubt, Oreskes and Conway documented the way that climate deniers sowed the seeds of doubt about climate change and successfully staved off implementations of mitigation measures. For the authors, the anticommunist ideology that had kept actors vigilant about government encroachment in the marketplace occupied a central place in climate denial (2014: 69). Ironically, this sort of ideology-informed calculation meant that preventative action was blocked, increasing the risk that disruptive climate disasters would eventually necessitate the suspension of democracy and legitimating the sort of heavy-handed authoritarian interventions that the conservatives most abhorred (2014: 52; 69).

An appeal to suspend democracy for the sake of survival can be found in The Climate Change Challenge and the Failure of Democracy, where Shearman and Smith argue that liberal democracy is incompatible with the urgent necessity to prevent catastrophic climate change. The vested interests of politicians, corporations, and media lie in continuing with business as usual and in keeping the public ignorant. Instead of bottom-up reforms to improve democracy and bring about sensible climate policies, Shearman and Smith see a transformation into authoritarian regimes as the only responsible way forward when faced with the extreme ecological stress of climate change. They point out that, as Plato foresaw, those in power in a democracy are seldom able to resist the demands of the populace for long, but as a mass, the populace is seldom able to focus on complex problems and to perceive threats that lie over the horizon. Hence, those able to see further—scientists, experts, and the knowledgeable— should be entrusted with steering the course while there is still time to avoid disaster. It is only under a benign authoritarian rule of the knowledgeable that a saner, fairer, and more rational means of weighing social goods against evils can be introduced (Shearman and Smith, 2007).

#### The public is an idiocracy. ‘Pressure’ cannot be productive.

Dr. Stuart Parker 20, Philosopher and Former Teacher who Lectured on Philosophy and Education at London's Institute of Education, South Bank University, Author of Reflective Teaching in the Postmodern World, “The Problem With Democracy — It's You”, The Article, 10/5/2020, https://www.thearticle.com/the-problem-with-democracy-its-you

So why is our democracy so unfit for purpose? Why is it that we can elect leaders who are little more than self-serving schemers, whose contempt for the electorate renders them incapable of giving straight, honest answers to even the most straightforward, reasonable questions? It’s not as if any of these qualities have been smuggled in under our noses. They are paraded before our eyes every single day. Nobody voting for Johnson or Trump could ~~be blind to the fact~~ [ignore] that they are serial liars. And yet they voted all the same. Why?

\*\*\*

Mencken was on to something when suggesting that the leaders we get, the leaders we deserve, closely represent something dark in the inner soul of the people. There’s no easy way to put this — the problem with democracy is the voters. The voters simply aren’t good enough to support a healthy democracy. They’re not up to the job. Now I know some will think: a snowflake-remainer-lefty-loser will always blame the voters just as a bad workman always blames his tools. But these tools are shot.

Consider this: a poll in 2005 found that 21 per cent of Americans believe in witches and 9 per cent that spirits can take control of a person. In 1999, 18 per cent believed the sun revolves around the earth — so much for “the science” — and in 2000, 31 per cent believed in ghosts, and increase of 20 percentage points since 1978.

By 2019, the year before Trump’s re-election attempt, significant numbers believed in the illuminati, Big-foot and a flat earth. Ghost-belief had risen to 45 per cent, as had the belief in demons. Belief in vampires stood at a fangtastic 13 per cent.

Britain has nothing to be proud of. While 33 per cent of us believe in ghosts and 18 per cent in demonic possession, a whopping 52 per cent of us believe that you can magically make a false claim true simply by writing it on the side of a bus.

In elective dictatorships where small margins have huge consequences we’d better get used to the fact that (possibly small) groups with stupid ideas and a lack of relevant knowledge and skills can have a disproportionate effect on the lives of the rest of us.

### 2NC---Causes War---Democracy

#### This is true in all scenarios, including against other democracies

Dr. Daina Chiba 21, Associate Professor of Political Science in the Department of Government and Public Administration at the University of Macau, Ph.D. in Political Science from Rice University, LL.M in Jurisprudence and International Relations from Hitotsubashi University, and Dr. Erik Gartzke, Professor of Political Science at the University of California, San Diego, PhD in Political Science from the University of Iowa, “Make Two Democracies and Call Me in the Morning: Endogenous Regime Type and the Democratic Peace”, 2/19/2021, https://dainachiba.github.io/research/make2dem/Make2Dem.pdf

We now turn to the results from the outcome stage, where militarized conflict initiation is regressed on democracy measures and other covariates. The univariate clog-log model 32 that ignores the endogeneity, shown in column (1) in Table 1, successfully replicates the standard, dyadic democratic peace finding that democracies are peaceful, though only toward other democracies. Note that, while individual democracy measures have either a positive or insignificant coefficient, joint democracy has a negative coefficient that overwhelms the positive coefficients of individual democracy measures in the univariate model. As a result, the univariate model produces a result that, while democracy may increase conflict against a non-democracy, it decreases conflict against a democracy.

To illustrate this, we calculate the average treatment effect of joint democracy for the challenger and for the target based on the univariate model. These effects are calculated by comparing the predicted probabilities of conflict initiation when changing the regime type of self (challenger or target) from non-democracy to democracy, holding constant the regime type of the other (target or challenger) as democracy. 33 Gray, hollow circles in Figure 4 show the treatment effects of challenger’s and target’s democracy. We can see that both effects are negative and statistically significant at the 95% confidence level.

Once we correct the endogeneity, however, the data no longer support such conclusions. In column (2) in Table 1, the negative coefficient for joint democracy no longer overwhelms the positive coefficient of challenger’s democracy. Challenger’s democracy now appears to increase conflict even against a democratic target. Red, solid circles in Figure 4 show the average treatment effects of challenger’s and target’s democracy, calculated from the trivariate model. The effect is positive and statistically significant for challenger’s democracy, although the effect is indistinguishable from zero for target’s democracy.

Whether we correct for endogeneity thus makes a significant difference in our estimates of the effect of joint democracy on conflict. The key to understanding why these changes occur lies in the estimated correlations between the error terms for different equations. The estimated error correlation between equations for conflict and challenger’s democracy, 12, is negative and statistically significant. This suggests that unobservable or unmeasured determinants of a country’s democracy make it less likely for that country to attack another country. A failure to control for such factors would generate a negative omitted variable bias, making it look as if challenger’s democracy has a pacifying effect on conflict behavior. On the other hand, the estimated error correlation between conflict and target’s democracy equations, 13, is indistinguishable from zero, suggesting that the endogeneity problem does not seem to operate for target’s regime type.

#### It's an empirical question, answered by statistical methods---failing to code based on exogenous variables corrupts their evidence

Dr. Daina Chiba 21, Associate Professor of Political Science in the Department of Government and Public Administration at the University of Macau, Ph.D. in Political Science from Rice University, LL.M in Jurisprudence and International Relations from Hitotsubashi University, and Dr. Erik Gartzke, Professor of Political Science at the University of California, San Diego, PhD in Political Science from the University of Iowa, “Make Two Democracies and Call Me in the Morning: Endogenous Regime Type and the Democratic Peace”, 2/19/2021, https://dainachiba.github.io/research/make2dem/Make2Dem.pdf

Before we review our approach in detail, it may be useful to explain why this type of analysis has not been pursued successfully in the past and what makes our effort different from other, broadly related projects. We are not the first to apply an IV framework (more specifically) or multi-equation models (more broadly) to the democratic peace. However, previous attempts suffer from two major problems. First, previous studies have typically used a dyad (country pair) as the unit of observation in analyzing conflict, which requires some summary measure(s) of democracy for a pair of countries rather than the state-level (monadic) democracy measure. 6 Use of a dyadic aggregate to represent regime type creates a discrepancy between the first stage regression (predicting democracy at the country level) and the outcome stage regression (predicting conflict at the dyad level). 7 We avoid this problem by using the directed dyad as the unit of observation in predicting conflict, distinguishing between the potential challenger and target in a dispute. This allows us to connect the first stage equations (predicting the challenger’s and target’s regime types) and the outcome stage equation seamlessly. Doing so has several benefits: the outcome stage model could directly include country-level covariates (such as challenger’s and target’s democracy) without having to convert them to a dyadic summary. This also allows us to estimate the system of equations jointly rather than relying on the “forbidden regression.” 8

Second, a more daunting challenge in applying an IV approach to democratic peace research is the difficulty of finding a plausible instrument for regime type — a variable that is strongly correlated with regime type but is unrelated to war. This is the challenge that has plagued empirical researchers in many fields. For example, a recent study of the effect of regime type on economic growth uses a diffusion-based measure of democracy (i.e., average value of democracies in a given region) as an instrument for democracy (Acemoglu et al. 2019). However, diffusion-based instruments such as this are unlikely to be a valid instrument, due to spatial spill-over, interdependence, and, most importantly, simultaneity (Betz, Cook, and Hollenbach 2018). Recognizing problems with spatial instruments, McDonald (2015) seeks to exploit the very discrepancy between country-level and dyad-level designs as the source of identification. His discussion, however, lacks a clear explanation as to why some determinants of regime type do not influence conflict. 9

We turn to a demographic variable — average female fertility rate in a given country — as a source of variation in regime type that is exogenous to international conflict. As we will argue below, a lower fertility rate is a strong driver of democratization. We will also present theoretical arguments and a series of falsification tests that support the claim that average national fertility rate does not directly influence international conflict.

### 2NC---Transition Wars

#### The move to democracy doubles the risk of quick conflict AND goes nuclear

Dr. Edward Mansfield 22, Hum Rosen Professor of Political Science and Director of the Christopher H. Browne Center for International Politics at the University of Pennsylvania, B.A., M.A., and Ph.D. from the University of Pennsylvania, and Dr. Jack Snyder, Robert and Renee Belfer Professor of International Relations in the Political Science Department and the Saltzman Institute of War and Peace Studies at Columbia University, Ph.D. in Political Science from Columbia University, BA in Government from Harvard University, Conflict After the Cold War: Arguments on Causes of War and Peace, Sixth Edition, Ed. Betts, p. 331-332

DANGERS OF TRANSITION

The idea that democracies never fight wars against each other has become an axiom for many scholars. It is, as one scholar puts it, “as close as anything we have to an empirical law in international relations.” This “law” is invoked by American statesmen to justify a foreign policy that encourages democratization abroad. In his 1994 State of the Union address, President Clinton asserted that no two democracies had ever gone to war with each other, thus explaining why promoting democracy abroad was a pillar of his foreign policy.

It is probably true that a world in which more countries were mature, stable democracies would be safer and preferable for the United States. But countries do not become mature democracies overnight. They usually go through a rocky transition, where mass politics mixes with authoritarian elite politics in a volatile way. Statistical evidence covering the past two centuries shows that in this transitional phase of democratization, countries become more aggressive and war-prone, not less, and they do fight wars with democratic states. In fact, formerly authoritarian states where democratic participation is on the rise are more likely to fight wars than are stable democracies or autocracies. States that make the biggest leap, from total autocracy to extensive mass democracy—like contemporary Russia—are about twice as likely to fight wars in the decade after democratization as are states that remain autocracies.

This historical pattern of democratization, belligerent nationalism, and war is already emerging in some of today’s new or partial democracies, especially some formerly communist states. Two pairs of states—Serbia and Croatia, and Armenia and Azerbaijan—have found themselves at war while experimenting with varying degrees of electoral democracy. The electorate of Russia’s partial democracy cast nearly a quarter of its votes for the party of radical nationalist Vladimir Zhirinovsky. Even mainstream Russian politicians have adopted an imperial tone in their dealings with neighboring former Soviet republics, and military force has been used ruthlessly in Chechnya.

The following evidence should raise questions about the Clinton administration’s policy of promoting peace by promoting democratization. The expectation that the spread of democracy will probably contribute to peace in the long run, once new democracies mature, provides little comfort to those who might face a heightened risk of war in the short run. Pushing nuclear-armed great powers like Russia or China toward democratization is like spinning a roulette wheel: many of the outcomes are undesirable. Of course, in most cases the initial steps on the road to democratization will not be produced by any conscious policy of the United States. The roulette wheel is already spinning for Russia and perhaps will be soon for China. Washington and the international community need to think not so much about encouraging or discouraging democratization as about helping to smooth the transition in ways that minimize its risks.

### 2NC---Nigeria Link

#### Spending on elections diverts from public services and locks in wealth inequality

Dr. Aloysius-Michaels Okolie 21, Professor in the Department of Political Science at the University of Nigeria, PhD in Political Science and MSc from the University of Nigeria, et al., “Does Liberal Democracy Promote Economic Development? Interrogating Electoral Cost and Development Trade-Off in Nigeria’s Fourth Republic”, Cogent Social Sciences, Volume 7, Issue 1, 4/28/2021, Taylor & Francis Online

PUBLIC INTEREST STATEMENT

The debate on the suitability of liberal democracy in supporting economic development in post-colonial African states has unabatedly continued to remain at the centre of current intellectual discourses and conversations. Although scholars seem to be focused on the endogenous constraints to the capacity of liberal democracy in generating the expected development outcome, specific attention is yet to be paid on how exorbitant spending on elections undermines human development in Nigeria. This study therefore argues that the electoral timetable of a 4-year tenure system renewable only once, which sustains exorbitant public expenditure on elections is antithetical to the human development drive of the Nigerian state. It diverts public spending, incapacitates the state from addressing the economic priority needs of the people, and deepens the gap between the rich and poor. Redesigning and retuning the content of liberal democracy in line with the demands, peculiarities and realities of the Nigerian state are highly recommended in the study.

#### That creates a time bomb that’ll inevitably implode stability---abandoning democracy’s key

Moses E. Ochonu 19, Cornelius Vanderbilt Chair in History and Professor of African History at Vanderbilt University, PhD and MA in African History from the University of Michigan, BA in History from Bayero University, Graduate Certificate in Conflict Management from Liscomb University, “Why Liberal Democracy is a Threat to Nigeria’s Stability”, Logos: A Journal of Modern Society & Culture, May 2019, <http://logosjournal.com/2019/liberal-democracy-is-a-threat-to-nigerias-stability/> [language modified]

The Real Cost of Democracy

Aside from the aforementioned financial cost of elections and patronage, other expenditures bring the recurring cost of the Nigeria’s 20-year democratic project into tens of billions of dollars, an expense that will sooner or later ~~cripple~~ [ruin] the country financially. Let me expatiate. A recent report confirmed what many Nigerians have long suspected about the remunerations of their elected executive and legislative leaders: Nigerian elected public office holders at all levels of government are the highest paid in the world.[5] Together with their string of assistants and advisors (who sometimes have their own paid advisors), Nigeria’s public officers gobble up at least half of the nation’s revenue and budgetary appropriations in legitimate rewards.

This prohibitive democratic overhead has left the country with a smaller pool of funds than ever to invest in the things that matter to Nigerians: roads, healthcare, schools, water, electricity, and food production. This odd reality of low returns on democratic investment is unsustainable. Something has to give.

What is being eroded is the very stability of the state, along with any trust that citizens still have in it. This is a proverbial ticking time bomb that will implode or explode if the trend continues, if this democracy endures. Twenty years since the return of civilian rule, it is not an exaggeration to say that not only has democracy not paid off for Nigeria but that it is now a threat to its stability and survival. This is a radical shift that has occurred stealthily and has thus been missed by the Western governmental and non-governmental actors that encouraged and funded democratic advocacy in the 1990s.

#### The two-party system creates polarization, social violence, and instability

Dr. Aloysius-Michaels Okolie 21, Professor in the Department of Political Science at the University of Nigeria, PhD in Political Science and MSc from the University of Nigeria, et al., “Does Liberal Democracy Promote Economic Development? Interrogating Electoral Cost and Development Trade-Off in Nigeria’s Fourth Republic”, Cogent Social Sciences, Volume 7, Issue 1, 4/28/2021, Taylor & Francis Online

The hitches and abnormalities characterising Nigeria’s electoral democracy are, no doubt, intrinsically linked to the institutionalised two-tenure renewable system. This tenure system was externally supported by the purveyors of liberal democracy and domesticated by the local accomplices solely for self-interest. In Nigeria, the winner-takes-all mentality as well as the high stakes usually associated with political offices heightens electoral contestations among the competing, polarised and distrusted ethnic nationalities who perceive political power as a means of advancing their peculiar economic interests. The struggle is usually intensified when it is obvious that access to state power guarantees an unfettered gateway to huge petro-dollar revenue. Indeed, the incumbent’s penchant for re-election often reinforces the tendency for divisiveness, violence, rancour and instability. For instance, the re-election bid of the then President Goodluck Jonathan in 2015 accounted for the deaths of 106 people while the election-related conflict in 2011 led to the deaths of 800 people and the displacement of 65,000 (Birch & Muchlinski, 2018; Harwood, 2019). The two-tenure system affects governance and policy responses since incumbent officials seeking re-election often devote a substantial part of their time and energy in politicking and grandstanding for a favourable outcome. This manifested in the 2015 and 2019 re-elections of Goodluck Jonathan and Muhammadu Buhari, respectively, in Nigeria when both leaders abandoned their jobs for campaigns. Also, given the monetised and winner-takes-all approach of Nigerian politics, incumbent candidates ruthlessly divert public funds for re-election campaigns. It drains the national treasury and redirects public expenditure to campaign funding rather than to human and capital development. A classic example is the ongoing investigation into the Office of the National Security Adviser which, at the interim, has revealed that the sum of 2.1 USD billion appropriated for procurement of military equipments was diverted and used to prosecute the 2015 general elections for the Peoples Democratic Party.

#### That implodes the country---autocracy solves

Dr. Moses E. Ochonu 20, Cornelius Vanderbilt Chair in History and Professor of African History at Vanderbilt University, PhD and MA in African History from the University of Michigan, BA in History from Bayero University, Graduate Certificate in Conflict Management from Liscomb University, “Liberal Democracy Has Failed in Nigeria”, Africa Is a Country, 2/7/2020, <https://africasacountry.com/2020/02/liberal-democracy-has-failed-in-nigeria> [language modified]

Liberal democracy’s capstone ritual, zero-sum elections, endow winners with all the rewards of victory—millions of dollars in licit and illicit earnings, local and international political visibility, and power. The loser, conversely, gets nothing. The result is a high-stakes version of what is called FOMO, or the fear of missing out, in American popular lingo. This fear of political exclusion in turn catalyzes desperation, which consistently and predictably produces messy, violent, and compromised elections.

In addition, since its return to civilian rule in 1999, liberal democracy has been an unacceptably costly enterprise for Nigeria. In 2019, the country spent about $670 million on a general election widely condemned as a sham. With budget financing increasingly steeped in external and internal debt, and given the fungibility of state funds, there is a depressing possibility that Nigeria is borrowing to fund elections and to finance its fledgling democratic institutions and processes. It’s a hefty price tag in a country where most people subsist on less than $2 a day. When this financial outlay is added to Nigeria’s notoriety for having some of the highest paid legislators in the world and for spending the national fortune to maintain a large army of elected and appointed civilian officials, the unsustainability of this “democratic” trajectory emerges in full relief.

It is not just the fiscal cost of elections and civilian administration that threatens to ~~cripple~~ [destroy] Nigeria. The social cost of this “democratic” adventure poses the most potent threat to the country. Plural, adversarial, and zero-sum elections have frayed the social fabric and undermined the cohesion of a notoriously fragile country. As mentioned previously, elections have been marked—and marred—by killings, displacement, scorched earth violence, and malicious manipulations. Electoral contests are little more than political warfare between factions of Nigeria’s political elite for access to the country’s resources.

The result of this charade has been a steady trend of voter apathy, represented by declining voter turnout, which stood at 35 percent in 2019. Nigerians are communicating their disillusionment with this iteration of democracy. Without urgent, profound reforms, the current path may destroy the country. It is no longer enough to argue that the current challenges are mere setbacks on the path to democratic maturity, or that escalating “democratic” tyranny is an aberration.

### 2NC---Nigeria Impact

#### It spills into the Middle East and South Asia---nuclear war

Walter Mead 13, James Clarke Chace Professor of Foreign Affairs and Humanities at Bard College, “Peace in The Congo? Why the World Should Care”, The American Interest, 12/15/2013, <https://www.the-american-interest.com/2013/12/15/peace-in-the-congo-why-the-world-should-care/>

The problem is that these wars spread. They may start in places that we don’t care much about (most Americans didn’t give a rat’s patootie about whether Germany controlled the Sudetenland in 1938 or Danzig in 1939) but they tend to spread to places that we do care very much about. This can be because a revisionist great power like Germany in 1938-39 needs to overturn the balance of power in Europe to achieve its goals, or it can be because instability in a very remote place triggers problems in places that we care about very much. Out of Afghanistan in 2001 came both 9/11 and the waves of insurgency and instability that threaten to rip nuclear-armed Pakistan apart or with trigger wider conflict India. Out of the mess in Syria a witches’ brew of terrorism and religious conflict looks set to complicate the security of our allies in Europe and the Middle East and even the security of the oil supply on which the world economy so profoundly depends.

Africa, and the potential for upheaval there, is of more importance to American security than many people may understand. The line between Africa and the Middle East is a soft one. The weak states that straddle the southern approaches of the Sahara are ideal petri dishes for Al Qaeda type groups to form and attract local support. There are networks of funding and religious contact that give groups in these countries potential access to funds, fighters, training and weapons from the Middle East. A war in the eastern Congo might not directly trigger these other conflicts, but it helps to create the swirling underworld of arms trading, money transfers, illegal commerce and the rise of a generation of young men who become experienced fighters—and know no other way to make a living. It destabilizes the environment for neighboring states (like Uganda and Kenya) that play much more direct role in potential crises of greater concern to us.

#### Boko Haram will get CBRNs---extinction

Dr. Bernard B. Fyanka 20, Ph.D. in History and Strategic Studies from the University of Lagos, Akoka Lagos Nigeria, "Chemical, Biological, Radiological and Nuclear (CBRN) Terrorism: Rethinking Nigeria’s Counterterrorism Strategy", African Security Review, Volume 28, Issue 3-4, 2/17/2020, Taylor & Francis Online

The end of the Cold War might have represented the end of mutually assured destruction (MAD), but it did not necessarily dispel the dangers of the nuclear age – in fact, to some extent the globalised proliferation of non-conventional weapons has instead escalated the possibilities for a nuclear attack being carried out. During the Cold War, the belligerents of any nuclear conflict would have been easily identifiable; however, in the post-Cold-War era, non-state actors and terrorist groups like Boko Haram have emerged as potential players in a new variety of nuclear conflicts that would entirely be based on terrorist models. The ominous possibilities for this new kind of warfare are indeed terrifying, and the rise in terrorist attacks around the globe enhances the likelihood of such an occurrence. Since 9/11, the body of academic literature on the threat posed by terrorists regarding weapons of mass destruction (WMDs) and chemical, biological, radiological and nuclear (CBRN) devices has increased. In Gary Ackerman and Jeremy Tamsett’s edited volume, Jihadists and Weapons of Mass Destruction, there is disagreement as to whether this threat is overestimated or underestimated.1 In recent times, however, ample ideological incentive for the use of CBRN devices has been provided by the likes of Abu Mus‘ab al-Suri – author of the ‘Global Islamic Resistance Call’ – who has stated that ‘[t]he aim of carrying out resistance missions and individual jihad terrorism “jihad al-irhabi al-fardi” is to inflict the largest human and material casualties possible on American interests and its allied countries’.2 This echoes the previous call of Grand Ayatollah Ahmad Husayni al-Baghdadi, who maintained:

If the objective and subjective conditions materialize, and there are soldiers, weapons, and money – even if this means using biological, chemical, and bacterial weapons – we will conquer the world, so that ‘There is no God but Allah, and Muhammad is His Prophet’ will be triumphant over the domes of Moscow, Washington, and Paris.3

For Boko Haram and other groups, there definitely exists a strong motivation for the use of WMDs, and the global reach of this thinking is not in doubt:

The globalization of the jihadist struggle has also led to an increased emphasis on Islamic identity. In combination with the ideological theme of revenge, the global struggle for Islamic identity has the potential to create a new jihadist cultic worldview in which its endorsers seek out WMDs because they represent the only means to significantly transform reality.4

Contextual scenarios in Nigeria strongly suggest that Boko Haram is one such group which has embraced the jihadist world view that endorses the use of WMDs. In this regard, the strengthened affiliation of Boko Haram’s splinter group – the Islamic State West Africa Province (ISWAP) – with the Islamic State of Iraq and Syria (ISIS) confirms their ideological persuasions. The motivation for Boko Haram to use such weapons is thus grounded in the recent use of chemical weapons by ISIS in both Iraq and Syria against both military and civilian targets.5 If ISIS is claiming ownership of a faction of Boko Haram as its West African province, it is likely to extend its tactics to its African allies.

In the light of the above, the use of WMDs by terrorists cannot be explained within the framework of orthodox terrorism theories. With this in mind, what Russell Worth Parker refers to as the ‘Islamic just war theory’ suitably anchors a discourse on terrorism and advanced weapons of war.6 Most theorists do not support a subjective theory of ‘just war’, but rather the traditional version that relies on Western ideas of morality and proportionality, as well as on motives for waging war.7 On the other hand, jihadist traditions reinterpret just war’s key tenet of proportionality to suit Islamists’ conflict rationale. According to the Western form of just war theory, wherein discrimination proves strategically impossible, any response should be proportionate to the action that compels it – hence, proportionality dictates that a military operation should not cause greater harm than the act that it was designed to counter or prevent.8 This proportionality argument is exemplified in the use of nuclear weapons in the Second World War; since casualty estimates for an invasion of Japan exceeded one million Allied lives, with similar estimates for Japanese military and civilians, a nuclear attack was preferable. Eventually, the actual casualties suffered from the bombing of Hiroshima and Nagasaki reached 200,000, which represents 10% of the casualties that would likely have been incurred if Japan had been invaded (see https://avalon.law.yale.edu/). In the light of this argument, justification for the use of WMDs by terrorist groups would rest on their interpretation of the extent of the damage caused by the military aggression and long-term imperialism of Western powers.

Fighting faceless enemies in a CBRN conflict, whether in West Africa or the Middle East, is hard to imagine. Enemies who can easily blend into the crowd and take on the face of ordinary civilians represent a nightmare scenario for security strategists all around the world. The risk of WMDs falling into the hands of terrorist groups is largely dependent on their ability to obtain weapons-grade nuclear material like uranium and plutonium, combined with gaining the capability to build and deploy weapons which make use of them. The global proliferation of nuclear material has made this possible today.

Global proliferation of fissile material

The collapse of the Soviet military-industrial complex ushered in a period of uncertainty regarding the security of nuclear material. Consequently, the risk of fissile material falling into the hands of terrorist groups – or into the hands of states that sympathise with or harbour such groups – increased considerably. Lax security at former Soviet nuclear facilities was widespread, making the theft of nuclear material possible. In the chaos that followed the Soviet collapse in the early 1990s, radioactive material was frequently stolen from poorly guarded reactors and nuclear facilities in Russia and its former satellite states. Police operations have intercepted shipments of Soviet nuclear material in cities as far away as Munich and Prague, and experts believe that large batches are still unaccounted for and most likely accessible to well-connected traders on the black market.9

Over 1800 metric tons of nuclear material is still stored in facilities belonging to more than 25 countries all around the world.10 Not all of this material is located in military stockpiles – in fact, most countries maintain civil stockpiles of plutonium for use in nuclear power reactors. The civil stockpiles in the United Kingdom (UK), India, Belgium, France, Germany, Japan and Russia add up to over 230 metric tons of plutonium. In spite of these enormous quantities, the UK, India, France, Japan and Russia have not yet reduced the reprocessing of plutonium for civil use. Although civil plutonium is not weapons-grade, it remains viable as a raw material that can be transformed through an enrichment process for use in a bomb. The United States (US) on the other hand has a comparatively small amount of civil plutonium because of its 1970 policy to suspend the separation of plutonium from spent nuclear fuel.11

About 25 kg of highly enriched uranium (HEU) is required to build a bomb – an insignificant amount in comparison to the global stockpile, which is in excess of 1.6 million kg. On the other hand, about 8 kg of plutonium is needed to build a bomb – a tiny fraction of the 500,000 kg global stockpile.12 Nuclear facilities that are relics of the Cold War era, especially those located in Eastern Europe, represent a high security risk. More than 130 nuclear reactors powered by HEU are operational in over 40 countries – the fallout of an early Cold-War-era programme in which the US and the Soviet Union helped their allies to obtain nuclear technology. Several other reactors have been shut down but may still contain nuclear fuel on site. In total, the world’s research reactors contain 22 tons of HEU – enough to build hundreds of nuclear bombs. The problem is that research reactor fuel tends to be stored under notoriously light security, making it a very vulnerable target for terrorists.13

In 2004, the US Government Accountability Office (GAO) published a report that details security lapses at civilian nuclear installations, citing a case in which the fences surrounding an unnamed foreign research reactor were in very poor condition and there were no guards securing the reactor building itself. In this report, Harvard expert Matthew Bunn explains that unlike the bulky and extremely radioactive fuel rods used in commercial nuclear power plants, research reactor fuel consists of small pellets that weigh only a few pounds each and moreover are easier to handle –a simple backpack can conceal several pellets.14 Naturally, civilian stockpiles are at greater risk of theft than those held in military installations. Consequently, the possibilities of such dangerous material falling into the hands of terrorists groups have become increasingly plausible.

Regarding military stockpiles, Russia and the US possess the largest amounts of weapons-grade plutonium – 100 and 150 metric tons, respectively. Diplomatic attempts aimed at reducing these stockpiles have resulted in an agreement for the two countries to dispose of 34 metric tons each via the method of turning the weapons-grade plutonium into fuel for nuclear power reactors. Although this agreement has not been effected yet, it is obvious given the above that the process may expose the material to greater risk of theft rather than securing it.15 On the other hand, in 2005 the US Congress eliminated the long-standing restrictions that were placed on the exporting of HEU to other countries for the purpose of manufacturing medical isotopes, which has also created new avenues for the proliferation of nuclear material through civilian use.16

Although the civilian use of nuclear material has increased the risk of its proliferation, the military facilities currently holding nuclear material around the world – especially in Russia – are also not well secured. Thousands of Cold-War-era tactical weapons are stored at very poorly guarded military installations, and most of these weapons are small and do not have electronic locks that prevent unauthorised usage.17 Since the collapse of the Soviet Union there has been no viable security strategy for securing the nuclear material contained in many of the former empire’s cities. During the Cold War era, the citizens of these cities had access to these facilities – and they still do, a problem further compounded by the fact that a strict inventory of the nuclear material contained in these facilities is not maintained.18

The likes of infamous arms dealer Leonid Minin (who was found guilty in a court of law for supplying weapons to non-state actors in African conflicts) are all too willing to do business with terrorists.19, 20 Arms dealers and smugglers all over the world are always seeking lucrative opportunities, and it is almost certain that some nuclear material has already been acquired by dangerous fanatics.

Several incidents in recent decades give every reason to believe that this is the case. In 1993, Kazakhstani authorities discovered HEU capable of arming 20 bombs in a building that was poorly secured.21 In 2006, Russian citizen Oleg Khinsagov was arrested in Georgia for carrying 100 g of HEU and attempting to find a buyer for what he claimed was many additional kilograms.22 In 2011, six men with 4 g of uranium were arrested by security forces in Moldova. Upon questioning, they claimed that the 4 g represented a sample of the product they were ready to market. They claimed to possess an additional 9kg, which represents one third of the quantity needed to create a nuclear weapon. The leader of this group and the North African buyer escaped.23 Four years before this incident, gunmen raided a facility in Pelindaba, South Africa; the details of the event are still shrouded in mystery.24

Efforts by terrorist organisations to purchase and use nuclear weapons continue unabated. The most high profile of these known efforts is that of Osama bin Laden, who in 2001 attempted to purchase a canister of uranium in Sudan for US$1.5 million. Intelligence reports claim that he also met with two Pakistani nuclear scientists, and sketches of nuclear weapons were found at an al-Qaeda training camp.25

From the foregoing, it is clear that there exists a robust and thriving black market in fissile material that seems to be tailor-made for use by terrorists groups. The International Atomic Energy Agency (IAEA) as at December 2015 had recorded in its trafficking database a total of 2889 incidents involving losses, thefts and/or attempts to traffic fissile material across international borders.26 This is an incredibly high rate of security lapses considering the security priority that nuclear facilities are supposed to possess. More pressing is the fact that the agency does not inspect every nuclear facility globally, and as such is not in a position to comprehensively enforce strict security and safety regulations. As a consequence of this, fissile material often goes missing and subsequently appears on the black market without being reported to the agency. Furthermore, several nations which maintain nuclear facilities do not possess the requisite resources to subject employees to the kind of extensive background checks that can ensure their trustworthiness for working at such high-security sites. In the absence of this screening, the likelihood of people with terrorist ties applying for jobs at nuclear facilities for the purpose of obtaining nuclear material is very high.

There is mounting evidence worldwide that increasing amounts of fissile material are being stolen and traded. Although the Russian government refuses to admit that it has lost any nuclear weapons, at least four Russian nuclear submarines have sunk, and it is believed that the warheads on board are yet to be recovered. The US on the other hand has admitted to losing a staggering 11 nuclear weapons.27

How can Boko Haram obtain nuclear material?

Boko Haram is one of the deadliest terrorist groups in the world. Since 2009, it has engaged with the Nigerian state in a lethal terrorism campaign aimed at toppling the secular structure and replacing it with an Islamist state. By May 2014 over 12,000 Nigerians had been killed in the insurgency,28 while one in five persons from Borno, Yobe and Adamawa states had been internally displaced. According to the 2017 Global Terrorism Index, Boko Haram ranks as the second deadliest terrorist group in the world, with an all-time high death toll of over 6000 in 2014 alone.29

With known ties to al-Qaeda, Boko Haram has an estimated annual income in excess of US$25 million.30 By 2017, Boko Haram had been forced to retreat from the large areas it had previously occupied in the north-east of Nigeria, driven back by the joint international military efforts of several countries in West and Central Africa. This created the need for them to reassert themselves. The likelihood of this group re-strategising and reconsolidating is high. Consequently, their acquisition of fissile material for the development and deployment of radiological ‘dirty bombs’ has increased in probability. The availability of this material on the continent and within Nigeria itself presents ominous opportunities for the group. Apart from large deposits of uranium ore found in Africa, several countries including South Africa, Morocco, Libya, Ghana, Egypt, the Democratic Republic of Congo (DRC) and Nigeria itself presently possess nuclear research reactors.31

The IAEA has reported no less than 12 incidents of natural uranium smuggling between 1995 and 2005 in Africa alone. In fact, illegal uranium mining at the Shinkolobwe mine in Katanga, DRC is presently a source of great concern. More importantly, this is where the source material for the Hiroshima and Nagasaki bombs was obtained.32 The proliferation of fissile material across the continent heightens the possibility of non-state actors like Boko Haram gaining access to it. Although there has only been one recorded theft of eight uranium fuel rods from a Kinshasa research reactor in 1997, the disturbing fact about this is that seven of the rods were never recovered.33

Within Nigeria itself, opportunities abound for terrorist groups like Boko Haram and other militant organisations to obtain fissile material for use in nuclear devices or dirty bombs. In 2004, Nigeria commissioned a 30-kW miniature neutron source reactor (NIRR-1) for the purpose of nuclear energy research.34 This nuclear facility is located at the Centre for Energy Research and Training at Ahmadu Bello University Zaria in the north of the country, where terrorist activities and Islamist extremism have been going on for centuries. The possibility of Islamist extremists infiltrating nuclear facilities and smuggling out fissile material has been an ongoing security concern for a number of years. An outright attack on a lightly secured facility is a second possibility that actually played out in 2007, when a nuclear research facility in Pelindaba, South Africa was raided by armed assailants, who breached its security perimeter and gained entry.35 Another concern is unsecured radioactive waste – namely 234 legacy sources presently located at the Ajaokuta Steel Company in Kogi State – that has not been disposed of and could easily be obtained by Boko Haram.36 To complicate matters further, the construction of a low to medium radioactive waste management facility at Nigeria’s Nuclear Technology Centre has been abandoned.37

Can Boko Haram build and use non-conventional weapons?

The poor state of nuclear security combined with the tenacity of Boko Haram makes Nigeria a prime location for the advent of nuclear terrorism. Knowhow on building a nuclear device is widely available, as is the key component, HEU, which can be found all over the world in dozens of military and civilian nuclear facilities – like the one at Ahmadu Bello University. Once Boko Haram has obtained enough HEU, a choice can be made between two types of nuclear device. The first is the gun-type mechanism, in which the HEU is smashed together to produce an explosion. The second type, which is more advanced, requires a chamber in which the HEU is compressed in a highly symmetrical manner in order to create an implosion. The gun-type mechanism is the more likely option for terrorist groups because it is simpler.38

In order to use the gun-type mechanism to activate a nuclear device, Boko Haram operatives would need to assemble a crude cannon that can smash HEU together – and the more highly enriched the uranium, the less advanced the weaponry that is needed. The viability of any terrorist group accomplishing such a task has been tested by US senator Joe Biden. In 2004 he asked scientists at three national laboratories to see if they could assemble the mechanical components of a gun-type bomb with commercially available equipment alone. A few months later, they reported back that they had succeeded.39 With over US$25 million in annual income, Boko Haram has the resources to obtain both the scientific knowhow and the materials needed to build and deploy a gun-type nuclear weapon.

Radiological dirty bombs

The threat of non-conventional weapons proliferation and terrorism goes beyond nuclear weapons – it also encompasses radiological dirty bombs. The raw materials used to create nuclear weapons are very dangerous; they contain highly radioactive substances that would pose a serious health hazard if dispersed in human populations using a detonation device. Plutonium and uranium could thus be weaponised in the form of a radiological dirty bomb, also known as a radiological dispersal device (RDD), which would cause widespread fatalities and cost billions of dollars in clean-up, evacuation and relocation operations.40

Terrorist groups like Boko Haram could easily build and use an RDD, given the widespread proliferation of fissile material – and more importantly given the dual-use materials that can produce the same radiological effects as fissile material from nuclear installations. Radiological dual-use materials from smoke alarms and medical services are among the most easily accessible; highly radioactive isotopes are in fact used in life-saving blood transfusions and cancer treatments in hospitals all around the world, including several in Nigeria. These isotopes include cesium-137, cobalt-60 and iridium-192, which can easily be used as base materials for a bomb or an RDD.41 The challenge is that most of the medical, commercial and industrial groups that handle these materials are not adequately equipped to provide the security needed to prevent them from being stolen. On the other hand, the lack of regulatory controls in many countries has led to thousands of instances of missing or stolen radiological material that cannot be accounted for. Recently, the James Martin Center for Nonproliferation Studies found in an alarming study that 170 incidents where nuclear or radiological material was lost, stolen or outside regulatory control occurred in 2014 alone.42

RDDs are viable weapons for terrorist groups like Boko Haram to pursue – and terrorist states have also attempted to obtain them. On 28 March 2002, Abu Zubaydah – a key al-Qaeda operative – was captured in Pakistan. He is widely believed to have told US investigators that al-Qaeda was ‘interested’ in building or obtaining a dirty bomb. Further evidence emerged on 8 May 2002, when Federal Bureau of Investigation (FBI) agents arrested Abdullah al Muhajir on charges of planning a radiological attack in the US at the direction of al-Qaeda operatives.

States that sponsor and support terrorist groups are likely to pass on fissile and radiological material to them. Iraq under Saddam Hussein is known to have sought radiological material for this purpose. In 1987, Iraq tested a bomb weighing 1400 kg that carried radioactive particles derived from irradiated impurities in zirconium oxide. A further 100 prototypes were designed from the casings of Muthanna-3 aerial chemical bombs, which were then modified to a 400-kg weight so that aircraft could carry more of them. It is likely that only 25 of these prototypes were destroyed, and that the other 75 were sent to the Al Qa Qaa State Establishment, a massive Iraqi weapons facility; their current status and whereabouts remain unknown.43

Chemical and biological weapons

The most commonly used non-conventional weapons are chemical or biological in nature. The long history of chemical and biological weapons usage dates as far back as 600 BC when, during a siege, Solon of Athens poisoned the drinking water of the city of Kirrha.44 More recently – starting with the use of mustard gas during the First World War – nations have acquired chemical and biological weapons easily, deploying them against enemies and their own citizens alike. For terrorist groups like Boko Haram, chemical and biological weapons are uniquely suited to their agenda and as such present very attractive alternatives to nuclear; they are extremely difficult to detect, cost effective and easy to deploy. Aerosols of biological agents are invisible to the naked eye, silent, odourless, tasteless and relatively easily dispersed. Most importantly they are 600 to 2000 times cheaper than other WMDs. Recent estimates place the cost of biological weapons at about 0.05% of the cost of a conventional weapon which could produce similar numbers of mass casualties per square kilometre.45

The proliferation of chemical and biological weapons has proved to be very fluid over the past century due to advancements in technology. Production is comparatively easy via the commonplace technology that is used in the manufacturing of antibiotics, vaccines, foods and beverages, while delivery systems such as spray devices deployed from airplane, boat or car are widely available. Another advantage of biological agents is the natural lead time provided by the organism’s incubation period (three to seven days in most cases), allowing the terrorists to deploy the agent and then escape before an investigation by law enforcement and intelligence agencies can even begin. Furthermore, not only would the use of an endemic infectious agent likely cause initial confusion because of the difficulty of differentiating between a biological warfare attack and a natural epidemic, but with some agents the potential also exists for secondary or tertiary transmission from person to person or via natural vectors.46

Unlike their nuclear and radiological counterparts, biological and chemical weapons have been used for terrorism by both state and non-state actors. The challenges faced in preventing the use of these weapons through international control mechanisms include the increasing availability of larger quantities of substances, ease of use and most especially advanced technological deployment facilities that portend a high risk factor to larger populations. Table 1 catalogues the use of biochemical weapons in warfare and by terrorists and other groups or individuals over the past century, offering concrete historical precedent and empirical grounds for the potential future actions of Boko Haram. The data shows consistent recourse to the use of these weapons, in spite of the chemical and biological weapons conventions outlawing them. It can be seen that from the 1970s onwards there has been an increase in the use of biochemical weapons by religious cults and terrorist groups in pursuit of their agendas. The rise of Boko Haram and its ISIS affiliation could lead to a future where the use of biochemical weapons is the norm rather than the exception.

As stated previously, the contextual scenarios in Nigeria that validate this prognosis regarding Boko Haram’s possible actions are strongly supported by their ideological persuasions. The fact that Boko Haram embraces a jihadist world view which endorses the use of WMDs is strengthened not only by its affiliation to ISIS through ISWAP but also by the similarities in its strategic modus operandi. Like ISIS, Boko Haram both believes in the slaughter of other Muslims who are deemed to be in cahoots with infidels, and advocates for the destruction of civilian populations – whether Muslim or otherwise – that are regarded as obstructing the advancement or creation of their caliphate.47 This was practically demonstrated by ISIS in Syria and Iraq when they used chemical weapons against both civilian and military populations, as shown in Table 1.48

Nigeria’s counterterrorism strategy

The central control measure for preventing nuclear terrorism is to ensure at the international level that nuclear material does not fall into the hands of terrorist groups like Boko Haram and other non-state actors in the first place. This is very difficult to achieve, given the lax security measures found at nuclear installations all over the world. Recognising the danger, the US under the Obama administration committed in 2010 at a nuclear security summit in Washington DC to securing all nuclear material within four years in an effort to prevent nuclear terrorism.49 Nigeria was a participant of this summit and is also committed to implementing the agreements that were reached. These attempts by the Obama administration followed up on the efforts embedded in the landmark 1987 Convention on the Physical Protection of Nuclear Material (CPPNM), which was meant to prevent nuclear material from being obtained by terrorists. The provisions of this convention were amended in 2005, and by 2010 the Washington summit had created the needed sense of urgency regarding the security of fissile material.50 Negotiations around the CPPNM started in 1979,51 and over the decades the growing proliferation of fissile material has combined with the increase in global terrorism to raise the profile of the issue of fissile material security. As of 2016, a total of 93 states including Nigeria had ratified the CPPNM, resulting in tighter security around the world at nuclear installations and border controls.

Nigeria has been engaged for decades in international efforts to control nuclear proliferation and terrorism. The country has ratified and acceded to over a dozen international instruments since 1963, including the Convention on Offences and Certain Other Acts Committed on Board Aircraft (1963), the CPPNM (1987), the Amendment to the CPPNM (2006) and the International Convention for the Suppression of Acts of Nuclear Terrorism (2007).52 At the level of global collective security, Nigeria is involved in implementing the United Nations (UN) Global Counter-Terrorism Strategy, which was adopted unanimously by the General Assembly in Resolution 60/288.53 At the regional and subregional levels, the counterterrorism strategies of the African Union (AU) and the Economic Community of West African States (ECOWAS) have been ratified and are in the process of being implemented. In pursuance of effecting these various international agreements, Nigeria has also instituted their National Counterterrorism Strategy (NACTEST), which was revised in 2016. Presently the country is also working with the UN Counter-Terrorism Implementation Task Force (CTITF) on projects designed to build community resilience against terrorism, enhance cooperation among law enforcement agencies and strengthen judicial institutions.54

Towards an integrated chemical, biological, radiological and nuclear (CBRN) counterterrorism protocol

The CBRN terrorism threat in Nigeria is both real and present. The country has one of the highest rates of terrorist activities in the world; in fact, according to the 2016 Global Terrorism Index, Nigeria ranked third among 163 countries, with a terrorism death rate of 16.8% of the global total.55 Although attacks declined in 2017, Nigeria still retained third place on the Global Terrorism Index.56 Recently, Boko Haram has initiated a comeback that has seen renewed attacks and the abduction of more girls from schools in the north-east of the country. Security forces have continued to engage the group on the frontlines in their forest bases; with the assistance of local and international joint task forces, much of the conflict has been shifted to more remote areas in the north-east. Although the government security forces have gained the upper hand in their frontal clashes with Boko Haram forces, by January 2018 the group had successfully carried out several brutal assaults, including one on UN and Doctors Without Borders staff, shifting their strategy back to traditional hit-and-run guerrilla tactics. During Easter of the same year, a single attack utilising 5 suicide bombers resulted in over 29 dead and 84 wounded.57

The likelihood that Boko Haram may begin to use CBRN weapons is increasing, and biological and chemical terrorism is potentially more difficult to prevent than conventional terrorist attacks. Since the latter part of the twentieth century, the Internet has contributed to the spread of chemical and biological weapons knowhow, thereby increasing the likelihood of Boko Haram being able to obtain not only the ingredients needed to create biochemical weapons but also the information needed to build and successfully deploy them. Some of the base materials for such weapons even occur naturally, like castor beans, which can be processed to produce the dangerous toxin ricin and deployed against unsuspecting populations. Furthermore, live strains of very dangerous viruses like Ebola can be found in high-tech research labs, like those at the African Centre of Excellence for Genomics and Infectious Diseases (ACEGID) at the Redeemer’s University Ede in Osun State. If Boko Haram were to secure this virus and weaponise it, the age of biowarfare would arrive in Nigeria – with deadly consequences. More importantly, the materials that are needed to create most chemical weapons exist in large quantities as dual-use materials that can be purchased on the open market and ferried into the country via forged end-user certificates.

The chemical and biological weapons conventions represent control structures geared towards the containment of these non-conventional weapons, and to a large extent state signatories like Nigeria have implemented a good level of the instruments contained in them; however, some nations still maintain secret stockpiles and have used them in recent conflicts, like Iraq against Iran and Kurdish dissidents in the 1980s and 1990s, and the Syrian government, which is presently using them against its civilian population.

On the whole, the counterterrorism measures put in place to deal with the aftermath of a chemical or biological attack have gained more credibility in the international community. Although there is no dedicated international inter-agency mechanism for coordinating the response to terrorism involving the release of toxic chemicals or biological agents, there are mechanisms that have evolved in the context of humanitarian assistance and emergency response after natural catastrophes, such as earthquakes; these include the Global Outbreak Alert and Response Network (GOARN), the World Health Organization (WHO), the Global Early Warning System (GLEWS), the Global Framework for the Progressive Control of Transboundary Animal Diseases (GF-TAD) and the International Food Safety Authorities Network (INFOSAN). The primary inter-agency mechanism that coordinates responses to emergencies involving the agencies mentioned above is the UN Disaster Assessment and Coordination (UNDAC).58 To further strengthen inter-agency coordination in the wake of a terrorist attack of catastrophic proportions, the UN CTITF is also focusing on planning for such an eventuality.

At the local level, several key aspects of Nigeria’s NACTEST are presently being utilised. The strategy is divided into five work streams:

* Forestall: Prevent terrorism in Nigeria by engaging the public through sustained enlightenment and sensitisation campaigns and deradicalisation programmes.
* Secure: Ensure the protection of life, property and key national infrastructure and public services, including Nigerian interests around the world.
* Identify: Ensure that all terrorist acts are properly investigated, and that terrorists and their sponsors are brought to justice.
* Prepare: Prepare the populace so that the consequences of terrorist incidents can be mitigated.
* Implement: Devise a framework to effectively mobilise and sustain a coordinated, cross-governmental, population-centred effort.59

Presently, the first three aspects of these work streams are receiving full attention. However, in regard to WMDs, the counterterrorism strategy is lacking a well-integrated CBRN protocol for engaging with the work streams for preparation and implementation. Nigeria currently handles issues relating to nuclear and radiological matters through two institutions: the Nigerian Atomic Energy Agency (NAEC) and the Nigerian Nuclear Regulatory Authority (NNRA). It is therefore expected that, given the growing CBRN threat level in the country, these agencies will collaborate with the Office of the Security Adviser to the President in order to initiate a proper CBRN counterterrorism protocol.

The NACTEST does not currently include a dedicated protocol for handling CBRN threats; Nigeria is however involved in nuclear security at the international level, which has primarily provided for capacity-building and human resources development. Activities in these areas include the gradual process of converting the miniature neutron source reactor in Zaria from using HEU to low enriched uranium (LEU), partnerships for nuclear and radiological security with the US Department of Defence (DoD) and the IAEA, establishing a nuclear security support centre in the country, reviewing the 2012 design basis threat (DBT) for protecting nuclear and radiological material, the development of a programme for locating and securing orphan legacy radioactive sources, training security officers, the installation of a radiation portal monitor at the Murtala Muhammed International Airport in Lagos in 2008 and the acquisition of three more monitors for other international airports in the country.60

An integrated CBRN protocol would fall under the preparation and implementation work streams of the NACTEST. The protocol should include a strategy for detecting CBRN agents in the wake of terrorist events, followed by disaster response and countermeasure initiatives to be carried out by security, medical and disaster response teams. Given the availability of advanced technology, the integrated CBRN counterterrorism protocol should also include the deployment of handheld radiological and biochemical detectors to high-risk areas, and security forces and disaster response teams should be trained in their usage. Embedding a standard protocol in the NACTEST on how to prepare for and respond to CBRN events is essential for repositioning counterterrorist activities in the country to meet the present threat level. The US and Canada along with the UK and most other European countries facing CBRN threats have already repositioned accordingly in order to accommodate this new reality.

Conclusion

Any terrorist attack involving WMDs is the ultimate nightmare scenario. Fortunately, at least some of these potential attacks are preventable. If and when the nuclear security summit achieves its goals, the possibility of a nuclear terrorist attack in Nigeria will be immensely reduced. Unfortunately, the likelihood of radiological, chemical and biological attacks is more difficult to regress, making it all the more vital to integrate a CBRN protocol into Nigeria’s counterterrorism strategy.

Preventing such a tragic event from occurring will require very close ongoing monitoring of the strategic manoeuvrings of Boko Haram. From its inception to the present day, the organisation has depended on the looting of military armouries to source most of its heavy weapons and equipment. It has built up an impressive arsenal in this manner and there is no indication that the group will stop using this highly profitable strategy, which could be further employed to obtain advanced CBRN weaponry from facilities that are vulnerable to being raided. The civilian facilities mentioned in this paper are at high risk of being targeted in this fashion; hence, the recalibration of Nigeria’s CBRN counterterrorism protocols should include a security framework that provides military security for facilities like the ACEGID in Osun State and the Centre for Energy Research and Training at Ahmadu Bello University Zaria. Lastly, although the IAEA has assisted in the conversion of Nigeria’s reactor from HEU to LEU,61 the availability of fissile material at the facility means that the risk of radioactive dirty bombs being created from looted material is still present.

### 2NC---Warming Link

#### Freedom to pollute and rights to consume guarantee overshoot

Dr. Chien-Yi Lu 21, PhD and MA in Government from the University of Texas, Austin, Visiting Scholar at Harvard University, Associate Research Fellow at the Institute of European and American Studies of Academia Sinica, Surviving Democracy: Mitigating Climate Change in a Neoliberalized World, Paperback Edition, 12/13/2021, p. 3-4

This pessimism stems from the unavoidable transition of capitalism from its expanding form to a stationary one under severe scarcity of resources, as “whether we are unable to sustain growth or unable to tolerate it…,it seems beyond dispute that the present orientation of society must change” (1980: 110, original emphasis). Social tensions will inevitably rise when scarcity-propelled stationary or even slow-growing capitalism renders infeasible the usual method of appeasing the lower and middle classes by further deepening the grab into the nature to improve their economic positions, leaving the diminishing of the incomes of the upper echelons of society the only option (1980: 102). Given the widespread belief that “centralized authority will cope with crisis and unrest more ‘successfully’ than less authoritarian structures” and the historic pattern in democracies where “the pressure of political movement in times of war, civil commotion, or general anxiety pushes *in the direction of authority*, not away from it,” (1980: 128–9, original emphasis) Heilbroner concluded that intolerable socioeconomic strains will eventually exceed the capabilities of representative democracy, leading governments of these societies to resort to authoritarian measures (1980: 106).

Similarly, Ophuls contended that under conditions of ecological scarcity, if individuals are allowed to pursue their self-interest “unrestrained by a common authority,” the result is bound to be “common environmental ruin” (1977: 151). Accordingly:

the individualistic basis of society, the concept of inalienable rights, the purely self-defined pursuit of happiness, liberty as maximum freedom of action, and laissez faire itself all become problematic, requiring major modification or perhaps even abandonment if we wish to avert inexorable environmental degradation and eventual extinction as a civilization. (1977: 152)

To him, the only solution is “a sufficient measure of coercion;” and “democracy as we know it cannot conceivably survive” (1977: 151–2).

In the same vein, Ophuls and Boyan (1992) talked about the crucial role that “ecological mandarins” must play under resource scarcity. Concurring with Robert Dahl’spoint that “a reasonable man will want the most competent people to have authority over the matters on which they are most competent” (Dahl, 1970: 58), Ophuls and Boyan emphasized that “under certain circumstances democracy *must* give way to elite rule,” and “the more closely one’s situation resembles a perilous sea voyage, the stronger the rationale for placing power and authority in the hands of the few who know how to run the ship” (Ophuls and Boyan, 1992: 209, original emphasis). Given that ecology is esoteric and that only those with talents and training are qualified as specialists, “a class of ecological mandarins who possess the esoteric knowledge” is required to run the “ecologically complex steady-state society” well. Such a society

will not only be ostensibly more authoritarian and less democratic than the industrial societies of today (the necessity of coping with the tragedy of the commons would alone ensure that), but it may also be more oligarchic as well, with full participation in the political process restricted to those who possess the ecological and other competencies necessary to make prudent decisions. (1992: 215)

#### Deep mitigation will never have popular support AND democracies have to be perfect across every country because pollution is trans-boundary---it’s try-or-die for a global political transition

Dr. Chien-Yi Lu 21, PhD and MA in Government from the University of Texas, Austin, Visiting Scholar at Harvard University, Associate Research Fellow at the Institute of European and American Studies of Academia Sinica, Surviving Democracy: Mitigating Climate Change in a Neoliberalized World, Paperback Edition, 12/13/2021, p. 2-3 [language modified]

The doubt about the ability of democracy to handle climate challenges is palpable from the intellectual Left as well. Eric Hobsbawm offered a threefold explanation for his pessimism. To begin with, many of the strategies needed to avoid climate change would be extremely unpopular and therefore difficult to implement in a democracy. As a result, even as “the impact of human action on nature and the globe has become a force of geological proportions,” “no support will be found by counting votes” for measures required for mitigating these problems. Moreover, given that nature is border-blind, even if voters of some democratic states were sensible, the political mechanisms available to human kind in the 21th century are “effectively confined within the borders of nation-states” and “dramatically ill-suited” to deal with problems lying beyond their range of operation (2007: 113). Finally, democratic national governments are not the only relevant organizational entities that can have an effect on an increasingly globalized and transnational world. “A growing part of human life now occurs beyond the influence of voters, in transnational public and private entities that have no electorates, or at least no democratic ones.” Thus, “[d]emocracy, however desirable, is not an effective device for solving global or transnational problems”(2007: 118).

This wave of academic literature that questions the compatibility of democracy with timely and effective climate mitigation resonates with works dating back to the 1970s that focused on the role of democracy in environmental conservation. In An Inquiry into the Human Prospect, Heilbroner set to answer, in a world plagued by problems such as rapid environmental degradation, “is there hope for man?” Writing in 1974, he highlighted that:

the amount of CO2 in the air is expected to double by the year 2020… sufficient to raise surface temperatures on earth by some 1.5o to 3.0o … bring[ing] sea levels above the level of the land in the populous delta areas of Asia, the coastal areas of Europe, and much of Florida. Long before that it is feared that the rise in temperature would have irreversibly altered rainfall patterns, with grave potential effects. (1980 [1974]: 72)

With the approaching of the depletion of natural resources, Heilbroner expressed deep doubt about the ability of the democratic form of government in ensuring the survival of [hu]mankind.

[C]andor compels me to suggest that the passage through the gantlet ahead may be possible only under governments capable of rallying obedience far more effectively than would be possible in a democratic setting. If the issue for [hu]mankind is survival, such governments may be unavoidable, even necessary. (1980: 130)

### 2NC---Warming Impact

#### It’s fast, causes extinction, and turns all other impacts---transitioning from democracy is key

Samuel Malm 20, Master’s Degree from Uppsala University, Disciplinary Domain of Humanities and Social Sciences, Faculty of Arts, Department of Philosophy, “Does Climate Change Justify a Global Epistocracy?”, Digitala Vetenskapliga Arkivet, 8/11/2020, https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1448606&dswid=8040

Climate change’s negative impact on humans is hardly something up for questioning. The World Health Organization believes that between 2030 and 2050 the effects of climate change will be an additional of 250 000 deaths every year; due to diarrhoea, malaria, heat stress and malnutrition.1 Accordingly, we can expect millions of deaths to occur, and the increased frequency of natural disasters will push the expected death toll even further. Additionally, the rising sea levels, and other environmental consequences, will cause an unprecedented flow of climate refugees towards areas that still are unaffected by the change. If we thought the impact was huge from the people fleeing the Syrian civil war, or the present corona pandemic, we should expect the climate disaster to be countless times larger. The pressure on societies and intergovernmental organisations will become tremendous, and we would be naïve if we did not expect this pressure to create additional suffering and death. What is then the cause of climate change? It is the result of anthropogenic acts, i.e., it is our current way of living that is causing the heating of the planet. Like a greenhouse, our planet is becoming hotter by the way that carbon dioxide traps more heat in the atmosphere, and by consequent increase the global average temperature. Additionally, it sets off other reactions that add positive feedback to the warming, e.g., creation of water vapour or the reduction of ice caps.

Now, this paper does not intend to demonstrate the truth of these claims, and if the reader is still sceptical about climate change, and its anthropogenic cause, numerous sources can justify and explain these facts better, for instance, rapports from IPCC. 2 Accordingly, I will assume these facts to be true, and that climate change will cause a state of affairs that contains a great deal of suffering and death; besides the possibility of civilisational destruction or human extinction. Thus, the circumstances are dire. So, let us summarise these detrimental effects into a single claim. Here it is:

State Of Affairs No Reduction: A state of affairs where climate change causes tens of millions of deaths, countless instances of additional human suffering, and the possibility of causing a collapse of human life as we know it.

This is what I will take as the effect of doing nothing to halt climate change. This then begs the question: If our current behaviour has such terrible consequences, why have we not implemented policies that prevent climate change?

1.2 What is the nature of the problem?

There are two ways to answer this question: we can give a historical description of how the issue has been misconstrued by interests that have a lot to gain from the status quo or, that we are dealing with a special type of problem that is particularly difficult for us to confront.3 In this paper I will only deal with the second dimension. Additionally, we can divide this dimension into two groups: first, we can describe how humans, by their very nature, are poorly endowed to deal with such problems as climate change, secondly, that the problem of climate change is what sociologists call a “wicked problem”. I will discuss the first aspect later on when describing psychological barriers. Now, I want to address characterising climate change as a wicked problem.

During the ozone depletion, discovered in the late seventies, the world’s states quickly came together and implemented the Wien protocol in 1985; a protocol that set down some policies for protecting the ozone layer. Subsequently, in 1987 the Montreal Protocol was implemented, that resulted in the complete removal of the chemical substances that created the ozone depletion.4 Why have we not seen the same collective action towards climate change? Well, first, we must clarify that in the case of the ozone depletion, the solution was much easier to implement; it took the removal of a few ozone-depleting substances. However, solving the problem of climate change is much more wicked (supposedly) and is said to fall under a specific type of problem posited by Horst Rittel in the late 1960s; wicked problems.5 These are deep problems that do not present you with a clear solution. Now, my initial definition of the problem seems to fly against this deepness, i.e., I have claimed there is a clear solution. However, those that see it as a wicked problem would contend that my definition is only one way to conceptualise the problem, and that there is a spectrum of definitions that seem more or less correct. What does this mean? Dale Jameison describes this well:

“There are many different ways of conceptualising the problem of climate change, each of which finds different resources relevant to its solution and counts different response as success and failures. If the problem is fundamentally one of global governance, then new agreements and institutions are what are needed. If the problem is market failure, then carbon taxes or a cap and trade system is what is required. If the problem is primarily a technological failure, then we need an Apollo program for clean energy or perhaps geoengineering. If climate change is just the latest way for the global rich to exploit the global poor, then the time has come for a global struggle for justice. This problem of multiple frames is characteristic of what are called “wicked problems.” And wicked problems are extremely difficult for political systems to address successfully.”6

I understand the appeal to find all these different ways to conceptualise the problem of climate change. However, I do believe we are doing ourselves a disfavour if we explain the lack of action in preventing climate change, and by consequent justify this inaction, by appealing to this problem of multiple frames. We should ask why it is of benefit to consider all these multiple frames when trying to stop climate change? I take it that the answer to this is our desire for finding the most accurate conceptualisation of the problem so that we can implement the most optimal solution. I believe this is wrong. At its core, we know the solution to the problem (reduce greenhouse gases) and we should accept the risk that we will implement a sub-optimal solution. Waiting around for the most accurate conceptualisation of the problem is counterintuitive, especially when we contemplate the risk it entails. The goal should not be too solve this problem of multiple frames by, for instance, taking steps to secure a unanimous acceptance of some particular framing of the problem, and by consequent enact the most optimal solution to climate change. Setting this as our aim is just to promote even more inaction; we need to accept a sub-optimal solution. I believe this desire to find the optimal solution which does not entail people having to accept a reduction in their current standard (no one gets elected by promising to reduce economic growth and causing other detrimental effects on their electorate) better explains our inaction then characterising climate change as a wicked problem. As Broome writes: “the economics and politics of climate change has concentrated on finding the best solution to the problem of climate change.”7 Meaning that we are looking for a solution without sacrifice — and by consequent choose business as usual.

Nevertheless, I believe we should not put too much importance on the wickedness of the problem. We know what it takes, and our technological achievements are well-equipped to deal with the problem (since it also has created the problem). Implementing some policies that reduce greenhouse gases is better, even if they are sub-optimal, then postponing taking any preventive measures.

Nevertheless, before closing this section, there is one more aspect of the problem of climate change that we ought to face; the need for immediate action. This aspect is of high importance, and we should not take it lightly; even though it fills a short space in this paper. Climate change has been going on for a long time, and year by year we increase the yearly outpour of greenhouse gases into the atmosphere, e.g., the last year (2019) we increase the outpour even more.8 Additionally, we are taking a risk when we do not know what positive feedback we are potentially setting off by not reducing the outpour. Accordingly, we need to accept the fact that the problem of climate change has the character of demanding our immediate action.

1.3 Clarifications

Before turning to the argumentation for this paper’s thesis, some clarifications are necessary. One of these is the role of “political authority”. When I argue that we have good reasons to prefer an epistocracy, I am arguing that we ought to accept the epistocratic method as the political authority and that this authority is legitimate, i.e., it has some moral justification for establishing a normative relation between it (political authority) and the subjects. There are several conceptual accounts of “political authority”, and I will use the right to rule account. This account portrays a more morally robust account of the relation between an authority and a subject. It essentially describes a kind of ideal political community where a deeper moral connection is present. 9 I believe this is what we think of when trying to evaluate the legitimacy that a political system, as in a state, have in coercing a population, and the subjects have a moral duty to obey the authority. This will be the conceptual definition of political authority. It has a moral right to rule and coerce people into obeying its political system of institutions that regulate the behaviour of its subjects and set out the course for where the political entity is heading, i.e., which state of affairs we realise in the future.

2. INTRODUCING THE SOLUTION

In this section, I will demonstrate why we ought to accept The Solution as a true normative claim, i.e., why we ought to take political action to prevent State Of Affairs No Reduction from coming into existence.10 Here is the claim:

The Solution: Reduce the global outpour of greenhouse gases to a level that has an excellent chance of causing the avoidance of State Of Affairs No Reduction.

One helpful way to characterise the normativity of The Solution is as a navigational problem. Where do we want our global society to be heading? I believe we can characterise the possible directions as a binary choice between The Solution and Not-The Solution. The second option I describe as follows:

Not-The Solution: Continue the outpour of greenhouse gases with the consequences that State Of Affairs No Reduction has an excellent chance of being actualised.

Now, even though The Solution contains multiple ways to get implemented, they all share the same normative content of causing a reduction of greenhouse gases in the atmosphere.11 Accordingly, it is this goal, and how it dictates the changes needed in our global institutions that are of such vital importance. By contrast, Not-The Solution shares the same normative content of taking no action that will prevent State Of Affairs No Reduction. Given this binary choice, I believe our intuition tells us that we ought to choose The Solution. What could speak in favour of Not-The Solution? Is there some option of Not-The Solution that we have a better reason to prefer? Maybe someone would contend that the uncertainty that surrounds climate change gives us good reasons to postpone taking any action, or, that other goals are much more important. Now, before addressing these concerns, perhaps our intuition becomes stronger (that we ought to choose The Solution) if I provide some scenario that could work as an intuition pump. Here is such a scenario:

*The Bus Ride*: So, picture, if you will, a bus that is on a direct course towards a large tree that will cause a great deal of suffering and death upon impact. Inside, the people are busy doing whatever they see fit, spending their time to make the bus ride as comfortable and meaningful as possible. However, there is a group of scientists that have analysed and investigated the devastating effect of this course, and that they need to perform some necessary action to avoid the tree. Perhaps they all need to drop what they are doing and give up some of their time jolting the bus enough so that the bus will miss the tree.

Accordingly, the world is the bus, the people on the bus is the world’s population, and the jolting of the bus is The Solution.12 I believe our intuition tells us that we ought to perform the necessary actions in order to prevent the bus from hitting the tree. What could possibly be more pressing? Do we have good reasons to do something else? Is the uncertainty of how bad the impact will be, and when it will occur, good reasons to not start jolting the bus?

Weighing different values against each other is tricky, and there are many scenarios where it is contentious if we should promote, for instance, equality or liberty. Some could argue that we ought to increase economic prosperity since it will maximise well-being for all humans; others will argue that securing peace takes priority; social justice; or environmental concerns. However, whatever we see as the road to the common good the implementation of The Solution is superior in its importance, because it secures that there will be a ground to put the road on. We will certainly not have social harmony in a state of affairs where climate disaster is present; the economy will suffer the consequences of the climatic impact on everything from production to transfer, and we have good reasons to believe conflict and tension will arise when the situation gets worse.

Now, perhaps some could say that it is immoral to demand that people make sacrifices to reduce greenhouse gases. I believe this is wrong. The implementation of The Solution will not demand a tremendous amount of hardship for the effect world population.13 Like Peter Singer’s case where we should sacrifice our clothes in order to save a child from drowning in a pond, we ought to sacrifice some niceties in order to save ourselves, and future generation from State Of Affairs No Reduction.14 Accordingly, the sacrifices necessary do not entail some morally questionable acts, i.e., reduce the level of greenhouse gases by killing off a portion of humans. I am talking about, for example, having to reduce flying to a necessary minimum, or, pay more in taxes so we can develop, and build, the technology that reduces the outpour of greenhouse gases, e.g., solar panels. Furthermore, it is the affluent world that will have to bear the biggest load of these necessary sacrifices. Especially, since the cause of climate change comes from the increased material standard enjoyed by people in affluent countries. They should, by consequent, accept the moral responsibility to combat the harm this wealth is causing, and going to cause. Or, put differently, the economic prosperity that has created this wealth is the cause of the climatic change, and the cost of emitting greenhouse gases has been an externality unaccounted for by either the consumers or the producers (a Pareto sub-optimal state of affairs). Additionally, it is common-sensical that if one group have very few resources, and another group has an abundance of resources, we should not solve a common problem by removing the few resources from the first group. The harm created by the amount of resources in the prosperous group should yield a good reason for them, bearing the bigger load.

Additionally, we should also accept that since anthropogenic acts cause State Of Affairs No Reduction, it leaves us with an additional moral reason to implement The Solution (leaving aside just the badness of State Of Affairs No Reduction). We bear the responsibilities of our actions, and these actions will harm countless future human beings.15 Even if we do not bear the responsibility of stopping climate change individually, we should not prevent our institutions from being reshaped in a way that solves the problem of climate change. I would even contend, if we are living in a democracy, we have a moral duty to use our political power (vote), so we take the necessary steps to implement something like The Solution.16 (Perhaps, this could also be interpreted as a reason for restricting universal suffrage (the democratic process) and justify an global epistocracy.) Possibly, in a counterfactual world where a non-anthropogenic event will cause a similar type of harm (for instance an impact by a meteorite), it could be argued that we have no responsibility to prevent this event since we are not the actors that create this event. I believe this is a weak argument for not preventing the impact from the meteorite. However, in the case of climate change that argumentation is not available since we are responsible for it.

One final thing is that The Solution is hardly a discriminatory or biased policy. Certainly, different groups will be affected differentially by the policy, and, as have been said, the affluent part of the world should bear the biggest load. However, the policy itself places no higher importance on any person or group. Satisfying, what Vandamme calls, a quality of (substantive) impartiality: “understood in a moral and substantive sense, as a property of public policies and of a political order, can be simply defined as not favouring some groups or individuals over others for morally arbitrary reasons.”17

2.1 Uncertainty of Climate Change

What then about uncertainty and the effect it has on the normativity of The Solution? Perhaps, someone would argue that since there is still uncertainty in the range of negative impact that climate change will have, and the lack of knowledge when things will start to get truly harmful, we can delay making any decision until the facts are in. I believe this is wrong. As Broome writes: “If you can costlessly delay a decision till all the information is in, you should delay it. But when delay itself is risky, it is not a sensible remark.”18 Choosing Not-The Solution and thus gamble in the hope that it will not have the consequence of suffering and death in order to avoid making a sub-optimal decision, that in hindsight is evaluated as unnecessary is, I believe, immoral and irrational.19 Accordingly, in the same way that it is rational to invest in a fire extinguisher, in case a fire starts in your house, it is rational to invest in the removal of the possibility of a climate disaster in the future. Why is this? I believe that Expected Value Theory is a good guide to adopt when facing uncertainty. Broome summarises this theory nicely:

“When the quantitative outcome of some process is uncertain, the expectation of the outcome is calculated as follows. Take each of the possible values of the outcome and multiply each by the probability of its occurring. Add up all of these products. The sum is the expectation. It is just a weighted average outcome, where the weights are the probabilities.”20

Even if it is a very small probability that climate change will have civilisational ending results, the great badness that this state of affairs constitutes should warrant our immediate action to avoid this scenario. Perhaps, there could be a case for not implementing The Solution if it would demand a large number of sacrifices, and by delaying this implementation we could remove additional uncertainty. For instance, what if people in The Bus Ride had to kill fifty per cent of the passengers, by throwing them off the bus, in order to avoid the tree. Certainly, given this tremendous sacrifice an argument could be had why we should delay implementing necessary precautions. However, even though the aggregation, of the small sacrifices every individual has to make, could become large, it does not constitute this tremendous sacrifice in The Bus Ride. The small sacrifices everyone have to make is easily overshadowed by the badness of State Of Affairs No Reduction. Accordingly, I still take it that we have better reasons to prefer The Solution than Not-The Solution even though climate change will always be immersed in uncertainty. We only have one opportunity to run this experiment, so we should not gamble with the outcome.

Nevertheless, I will not try and persuade the reader more of the badness of State Of Affairs No Reduction and that we ought to implement the Solution. Possibly, the discussion of the next section will bear some support for the accuracy of The Solution.

3. THE ANSWER

What we then must ask ourselves is: Which process for collective decision-making do we have reasons to believe will successfully implement The Solution? We could start with an unhelpful answer: The method that has the best chance to implement The Solution. Which method is this then? Here we get to the core of this paper’s thesis. I will call the answer to this question simply: The Answer. Here it is:

The Answer: Given that we ought to implement The Solution, and by consequent avoid State Of Affairs No Reduction, we have better reasons to prefer some form of global epistocracy, than a global democracy.

#### It’s the only existential risk

Samuel Miller-McDonald 19, PhD Candidate in Geography and the Environment at the University of Oxford, “Deathly Salvation”, The Trouble, 1/4/2019, https://www.the-trouble.com/content/2019/1/4/deathly-salvation

A devastating fact of climate collapse is that there may be a silver lining to the mushroom cloud. First, it should be noted that a nuclear exchange does not inevitably result in apocalyptic loss of life. Nuclear winter—the idea that firestorms would make the earth uninhabitable—is based on shaky science. There’s no reliable model that can determine how many megatons would decimate agriculture or make humans extinct. Nations have already detonated 2,476 nuclear devices.

An exchange that shuts down the global economy but stops short of human extinction may be the only blade realistically likely to cut the carbon knot we’re trapped within. It would decimate existing infrastructures, providing an opportunity to build new energy infrastructure and intervene in the current investments and subsidies keeping fossil fuels alive.

In the near term, emissions would almost certainly rise as militaries are some of the world’s largest emitters. Given what we know of human history, though, conflict may be the only way to build the mass social cohesion necessary for undertaking the kind of huge, collective action needed for global sequestration and energy transition. Like the 20th century’s world wars, a nuclear exchange could serve as an economic leveler. It could provide justification for nationalizing energy industries with the interest of shuttering fossil fuel plants and transitioning to renewables and, uh, nuclear energy. It could shock us into reimagining a less suicidal civilization, one that dethrones the death-cult zealots who are currently in power. And it may toss particulates into the atmosphere sufficient to block out some of the solar heat helping to drive global warming. Or it may have the opposite effects. Who knows?

What we do know is that humans can survive and recover from war, probably even a nuclear one. Humans cannot recover from runaway climate change. Nuclear war is not an inevitable extinction event; six degrees of warming is.

## NATO Advantage

### 1NC---Conventional Deterrence Turn

#### European security cooperation is stable, but has shifted to the EDI to deter Russia---plan trades off, undermines conventional deterrence

Michael J. Mazarr et al 22, senior political scientist at the RAND Corporation. "Security Cooperation in a Strategic Competition" Research Report. <http://www.rand.org/t/RRA650-1> //pipk

Security Cooperation Efforts in Europe Emphasize Reassuring U.S. Allies European partners have consistently received approximately 26 percent of all U.S. security aid, but there has been a shift since 2014 in the type of aid these partners have received. Specifically, more attention has been devoted to developing conventional capabilities to deter Russian aggression. Eastern European states that border Russia, particularly Ukraine, received $1.1 billion from 2014 to 2019.18 Georgia, Latvia, Lithuania, and Estonia also received some funding through the European Deterrence Initiative. However, of the billions of dollars designated for the initiative, only a small portion supports building partner capacity. The initiative was designed primarily to support U.S. force presence, infrastructure, and exercises; as a result, DoD does not formally categorize European Deterrence Initiative funding as security aid.19

Over our period of study, U.S. military sales have increased for both highly capable allies and newer North Atlantic Treaty Organization (NATO) partners in Europe. Among the top weapon purchasers, the United Kingdom, Italy, and Germany are purchasing advanced aircraft, unmanned aerial systems, and missiles through the FMS and DCS programs. Poland and Romania are acquiring Patriot air-defense systems, and Slovakia is purchasing F-16 aircraft through FMS.20

The focus of U.S. education and training efforts in Europe has also been on conventional military capabilities funded by FMS. Germany, the Netherlands, Italy, Romania, and Poland are the top recipients of these security cooperation activities.21

Furthermore, U.S.- and NATO-sponsored exercises in Europe are increasing in number and size. These exercises, which focus on improving interoperability for conventional operations, include Saber Guardian (a U.S.-sponsored exercise with 25,000 service members from 22 allied and partner nations) and Trident Juncture (a NATO-sponsored exercise with 50,000 participants from NATO and partner countries).22 NATO arrangements afford the United States a high degree of access in Europe. Of the 51 countries in the EUCOM AOR, 45 have multilateral SOFAs through NATO or the Partnership for Peace program, and there are 126 acquisition and cross-servicing agreements that apply to the region.23 The majority of USAF armament agreements and airmen in personnel exchanges are with European countries, and most personnel exchanges through the USAF’s Military Personnel Exchange Program are with the United Kingdom. Countries in EUCOM’s AOR received $27 million in Overseas Humanitarian, Disaster, and Civic Aid support, divided across several Eastern European states; Ukraine received $4 million, the highest amount.

### 1NC---Cyberwar Good

#### Deterrence and norms are effective at preventing large-scale attacks

David **Lonsdale 17**, School of Law and Politics, University of Hull, Cottingham Road, Lonsdale, David J. “Warfighting for Cyber Deterrence: A Strategic and Moral Imperative.” Philosophy & Technology, Feb. 2017. CrossRef, doi:10.1007/s13347-017-0252-8.

3.4 The Failure of Cyber Deterrence? The potency of cyber deterrence is difficult to judge. This is partly because there exists no consensus on what constitutes an act of sufficient cyber aggression. Therefore, it is not entirely clear what is to be deterred. Where exactly the threshold for response should be will be discussed in section three of this paper. For now, we can state that low-level nuisance attacks are a daily occurrence. For example, U.S. military networks are probed and scanned millions of times each day (Work 2015, 1). Similarly, acts of cyber espionage are reasonably common. However, what is also evident is the lack of major cyber attacks. For a while, Stuxnet, Wiper, Shamoon and Bronze Soldier appeared to signal the rise of cyber attack as a potent new instrument of policy. However, medium to large-scale attacks have essentially dried-up. Indeed, reflecting the empirical evidence, and marking a shift in tone, in his September 2015 testimony to the Senate Armed Services Committee, Director of National Intelligence, James Clapper, talked down the possibility of an ‘electronic Pearl Harbor’. Instead, he focused on ongoing ‘low-to-moderate’ level threats (Clapper 2015, 2). What does this all tell us? Is deterrence working? If one considers low-to-moderate threats as deterrable, then the answer would seem to be no. From this perspective, and according to some policy makers, deterrence is already failing. In a 2015 Senate Armed Services Committee Hearing, Chairman John McCain was scathing in his assessment: ‘Our adversaries view our response ... as timid and ineffectual. Put simply, the problem is a lack of deterrence. The administration has not demonstrated to our adversaries that the consequence of continued cyber attacks against us outweigh the benefit.’ (Takala 2015) However, if we take the view that cyber deterrence should really concern itself only with large-scale attacks, the picture is more positive. Indeed, Valeriano and Maness (2015) have identified considerable levels of restraint in state cyber behaviour. This could be due to a lack of confidence in the strategic utility of cyber attack. It may also reflect the development of norms against aggressive forms of cyber behaviour and the efficacy of deterrence. Indeed, norms increasingly form part of ‘complex deterrence’, within which military and non-military elements operate together. In cyberspace, although a settled understanding of universal rules of behaviour is still lacking, norms appear to be crystalising around acceptable forms of intrusion rather than a blanket non-use position (Stevens 2012, 25). This may explain the continuance of lowlevel probes whilst large attacks have trailed off.

#### Low-level attacks are stabilizing- no escalation

Yoo, 17—Emanuel S. Heller Professor of Law, University of California, Berkeley, School of Law (John, “Embracing the Machines: Rationalist War and New Weapons Technologies,” 105 Calif. L. Rev. 443 (2017), dml)

New weapons technologies can help overcome the obstacles of imperfect information. Coercive measures can signal political will, the value placed on the resources at stake, or military capabilities that could influence the outcome of a broader armed conflict. The more costly the signal, the more credible the information becomes. A nation's leader can make a threat of war and send military forces near disputed territory or a potential conflict zone. Deployment eats up resources that would go to waste if the nation is bluffing and incurs "audience costs" domestically if the leader backs down."' Escalating steps of force will provide the opportunity to send more precise signals that gradually consume more resources, reveal more military capability, and edge closer to war. With more avenues to credibly signal capabilities, there are more opportunities to reveal reliable, private information, and the likelihood of bluffing is reduced. While new weapons technology may produce more opportunities for violence, it can signal nations' capabilities and therey lead to peace settlements rather than war.

Limiting the ability to deploy new weapons technologies might make war more harmful. A ban could narrow the range of targets and the means of coercion to produce more destructive signaling and ultimately more lethal conflicts. One nation may want to send a signal during a crisis that inflicts a precise cost on its opponent. With a broader set of targets and more levels of harm, the nations can send more discrete signals in the bargaining process. If nations limit their signals to conventional attacks on military targets, they will have to employ more destructive levels of force. They might develop even more devastating kinetic weapons to produce the same effects as the precision offered by cyber or robotic weapons. Limits on new weapons technology might even destabilize crises by encouraging nations to use offensive weapons early in a crisis because they might themselves be vulnerable to attack. 15 4

New weapons technologies can more easily send specific signals that advance the bargaining process toward settlement. Cyberweapons, for example, can be used to shut down an opponent's financial markets or transportation and communication networks for a limited time. During the Kosovo War, the United States Air Force achieved a similar result by dropping graphite on Belgrade's electrical grid, which temporarily disabled power to Serbia's capital city. While NATO claimed that the disruption in electricity undermined Serbian military operations, the attack on the electricity grid also sought to pressure Serbian civilians against supporting the Milosevic regime.15 5 While such an attack would violate the ban on targeting civilian objects set out in the Additional Protocol I of 1977 to the Geneva Conventions, it can send a signal that may cause less loss of life and destruction than an attack on a hardened military target using kinetic weapons. Cyberweapons, in particular, present opportunities to send a more nuanced range of signals during interstate crises.' 5 6 Nations can use cyberweapons to attack each other's armed forces more precisely, and hence reduce direct casualties to both military personnel and civilians. In a contest over Taiwan, for example, China could use cyberattacks to disable communications between the Pentagon and the U.S. Seventh Fleet. These cyberattacks can inflict fewer, more directed costs than kinetic attacks. Cyberweapons' precision can reduce collateral harm to civilians by targeting only military communications. While cyberattacks can cause widespread harm, such as cutting water and electricity services to civilian populations, they still offer more precise and controlled power than kinetic weapons.

One might respond that some type of international regulation could forestall long-term harms from cyber conflict that might outweigh the benefits of credible signaling. Cyberweapons, for example, might also make possible new types of harms that did not previously appear in warfare, such as China's alleged theft of the U.S. personnel management database or North Korea's entry into Sony's network. Or cyberwarfare might open up a means for a faster escalation of hostilities. But even if true, these costs have to compare to existing means of signaling, which would depend on the use of conventional, kinetic weapons and their accompanying destruction and loss of life. They would also have to balance against the costs of cutting off a set of communications, which might impede peaceful bargaining.

Even if nations could overcome informational asymmetry, the international system's anarchy creates a second, more difficult, obstacle to cooperation. While nations may understand that avoiding war is mutually advantageous, they may not trust each other. The enforcement problem is acute in situations where a settlement changes the status quo between states, or where rapid changes are already affecting the balance of power."' One nation may find it difficult to trust the other to keep a promise if the latter will become even more powerful as a result of the agreement.

Information problems, for example, do not seem to explain the problems with ending internal armed conflict or long wars. Internal armed conflicts between a government and a rebel group often go on for years-sixteen years, on average.15 8 Over the course of the war, both sides acquire information about each other's goals, resources, and will. Even with far more information than at the war's outset, the parties often choose to fight rather than reach an agreement. This may well be due to lack of enforcement mechanisms. A settlement may put one of the two parties in a better position than when the fighting continues. A rebel group may gain breathing space where it can regroup, or the government may restore its authority in lost territory. One side cannot be confident that the other will not take advantage of its new position to break the agreement and take even more resources in the following year.

A hypothetical territorial agreement between the United States and China over Taiwan illustrates the difficulties of securing enforcement of a settlement amidst a shifting balance of power. In the first time period, the United States protects an independent iTaiwan. The United States has a greater probability of prevailing in any conflict with China because of its larger navy, air force, and forward bases in Korea, Japan, and the Philippines. In the second time period, China's economy has boomed, which translates into greater military power. China gains a higher probability of winning in a war with the United States. In this period, China and the United States agree to divide Taiwan in the middle because, with full information, they both estimate their chances of winning a war at fifty-fifty. China's gain of territory on Taiwan, however, gives it a greater than 50 percent chance of prevailing in the next time period because it now has a land base on the island itself. China's prospects will also improve in the third time period because of faster economic growth and military spending rates.

Under these conditions, the United States will have little confidence that China will keep its agreement in the second time period. An agreement will endow Beijing with an even greater advantage in future time periods, which will encourage it to revise the division of Taiwan further in its favor. China's conduct under its agreement with the United Kingdom over Hong Kong illustrates the problem. In December 1984, China achieved a superior military position relative to the United Kingdom in any conflict over Hong Kong. In 1982, for example, China spent $49.5 billion on defense whereas the United Kingdom spent $27.4 billion (they were the third and fourth largest spenders, respectively, with the Soviet Union first at $257 billion and the United States second at $196.3 billion). 59 But, much of the British military was deployed in Europe as part of NATO, and China's proximity to Hong Kong created a strategic advantage. To guarantee a peaceful transfer of power, Beijing promised in an agreement with London that Hong Kong would continue to enjoy an independent political system. Today, it appears that China is reneging on this negotiated agreement; the Communist Party has installed unpopular political leaders in Hong Kong to extend the mainland's power over the territory. In the twenty-first century, the United Kingdom has little military ability to prevent Beijing's revision of the deal. The 1984 handover agreement could not withstand a serious shift in the balance of power between China and the United Kingdom.

Cyberwarfare might provide an unexpected way to increase the ability of nations to commit to the terms of an agreement. In order to make a reliable agreement, a nation has to be willing to suffer a serious loss if it fails to perform, much like a borrower putting up property as collateral for a loan. But nations may have difficulty offering territory or resources as a security deposit on their treaty promises. A nation, however, could leave some valuable resource deliberately vulnerable to attack by cyberassault from its treaty partner. It could ensure that the cyber defense of the resource could only be overcome by capabilities in the hands of the other nation. If one state violated its international agreement, the other state could use cyber weapons to destroy the resource. This would be the twenty-first century equivalent of the ancient and medieval practice of sending the children of aristocratic families to foreign nations to serve as hostages, or the more recent concept of mutually assured destruction during the Cold War. Due to the lack of enforcement, however, states could never be certain that a nation would not renege even on these guarantees-a nation could always remove the vulnerabilities or suddenly deploy new defenses. But these expensive signals of commitment could improve the ability to cooperate beyond matters as they stand now.

A critic might argue that without international regulation of these new technologies, the risk to civilians will increase. Nations at war, however, will have an incentive to distinguish between military and civilian targets to the extent allowed by the capabilities of weapon systems. Rational nations should seek to contain the harms of war in order to maintain the conditions for peace and to preserve the value of the civilian economy in the postwar period. 160 Defenders in a war do not want to kill their fellow citizens or harm their own territory, although they might destroy civilian property to prevent it from falling into enemy hands. Invaders will have no interest in ruining the object of their aggression. Reducing civilian casualties may also encourage an end to conflict. Targeting civilians and destroying nonmilitary resources may harden nations at war and make a diplomatic compromise more difficult. The unexpected carnage of World War I, for example, made a peace agreement restoring the status quo to pre-August 1914 politically impossible for both the Allied and Central Powers.

Nations, moreover, have long pursued indirect coercion against civilian populations in war. They have often turned to economic sanctions to conduct hostilities short of direct armed conflict, or in conjunction with active hostilities. In World Wars I and II, of course, the Allies conducted economic warfare against Germany and its allies by levying a blockade of both military and civilian shipping. 161 After the wars, the UN Charter even expressed a preference for such tactics by authorizing the Security Council to impose "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication" in the case of a threat to international peace and security.

While nations such as Great Britain and the United States have argued in the past that embargos blocked only goods that might contribute to the enemy military, this seems difficult to sustain in the case of the complete embargoes that prevailed during the World Wars. Instead, economic warfare serves the same objectives as the approach described here for cyber and robotic weapons. First, new cyber and robotic weapons provide nations with a way to send signals in international bargaining through the gradual escalation of coercion short of outright hostilities. Second, embargoes pressure civilian populations to change the policies of their leaders, or even the leaders themselves. Perhaps cyber and robotic weapons, when employed as steps in the escalation of force, will also be understood as more akin to economic than kinetic warfare.

A rationalist approach to war also provides an answer to the broader critique of the new weapons technologies as facilitating war. Recall that some UN officials and scholars share the concern that drones and cyberweapons will encourage states to wage war more often. Critics argue that these weapons remove a nation's soldiers from the battlefield, theteby emboldening leaders to choose force more frequently. But, understanding war as a bargaining failure reveals the importance of signaling to resolving international disputes. New weapons create more opportunities for signaling, which allows nations to communicate their intentions and capabilities more effectively. Greater signaling should allow nations to share more information, which on the margins will lead to more international deals and therefore an overall reduction of major wars. Ironically, an effort to ban new weapons may well produce more war, not less.

#### Chinese A2/AD dependence on cyberweapons gives the US an advantage because we’re better at shutting down their systems than they are at targeting ours. Having cyber options give them false confidence and decreases their emphasis on conventional capabilities.

Jon **Lindsay 15**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies., Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security, vol. 39, no. 3, Jan. 2015, pp. 7–47.

the downside of “informatization” China’s ambition to become a world-class military power will lead the PLA to become more like the U.S. military in its dependence on networks and space assets. This modernization will undermine the asymmetry of vulnerability thought to make cyberweapons so dangerous to the United States and instead put some of the PLA’s own most sophisticated systems at risk. PLA antiaccess capabilities against U.S. power projection also include antiship ballistic missiles, cruise missile boats, antisatellite weapons, and ªfth-generation aircraft. The PLA requires traditional forces, moreover, for other missions that might require warªghting, military operations other than war, or coercive diplomacy (a role ill-suited for secret and intangible cyberweapons). China’s goal of “winning local wars under the conditions of informatization” requires the PLA to “enhance [its] warªghting capabilities based on information systems.”94 This transformation into a modern “informatized” force, inspired in no small part by American RMA ideals and force structure, entails greater reliance on C4ISR systems and computer networks. Yet China’s pursuit of the promise of the RMA will also reveal its liabilities. In imagining and planning for a potential war with the United States, the PLA has to worry about the demonstrated ability and willingness of the U.S. military to conduct cyber operations on the battleªeld (in Iraq and Afghanistan) and in covert action (e.g., the Stuxnet attack). If cyberwarfare is as effective as Chinese writers believe it is but they underestimate the costs of mastery, then the PLA is doubly disadvantaged. Chinese attacks can be expected to be less skillfully coordinated against more robust U.S. defenses, and vice versa. The United States already has, while China still struggles to develop, the institutional complements and experience required to plan and control cyber operations in synchrony with the larger battle. Meanwhile the fear of cyberwarfare has prompted considerable U.S. military investment in network protection, active cyber defense measures (e.g., counterintelligence deception and “hack back” counterattack), and exercises in cyber-degraded conditions. The vaunted asymmetry of cyberwarfare, usually posed as an advantage for the weaker power, in fact runs in the opposite direction, giving the stronger and more experienced force the advantage.95 If the military utility of cyber- warfare is actually more limited than Chinese doctrine writers seem to believe, then conventional considerations about military effectiveness (e.g., the balance of power as well as skill in combined arms warfare and joint operations) should be expected to dominate strategic calculation and operational interaction in any conºict.

#### If they refocus on conventional weapons, they’ll beat us straight up.

Col Michael W. **Pietrucha 15** (Col Michael W. “Starbaby” Pietrucha, 10/5/15, "Re-Fighting the Wrong War: Applying the Pacific War Template Against China," Leading Edge, accessed 2-12-2017, https://leadingedgeairpower.com/strategy/re-fighting-the-wrong-war-applying-the-pacific-war-template-against-china/)

Military organizations are often accused of fighting the last war. In the case of the US Air Force, the war in question is DESERT STORM, the last unambiguous US victory and a major milestone in the development of airpower. The Gulf War was a major success for airpower, demonstrating effective applications of stealth, precision, and electronic warfare. But the war was fought with overwhelming logistical, numerical and technological superiority against an adversary that was geographically isolated, poorly trained, badly equipped and ineptly led. It is unlikely that we will operate from such a position of advantage again. DoD planners should give up on the fantasy of a short, decisive war against the People’s Republic of China – any short decisive war involving the PRC is likely to end in a PRC victory. The lessons from the Gulf War should be applied to future conflicts with caution, especially if the adversary is China. In a potential conflict with China, it is the US that is geographically and numerically disadvantaged, and Chinese military development for the past two decades has been organized around one key principle – that the US would not be allowed to repeat DESERT STORM. The DoD summarizes the Chinese approach under an “anti-access, area denial” (A2AD) label, but is overly focused on finding technological means to operate in the A2AD environment in order to attempt a repeat of the Gulf War’s air campaign. China is perhaps the least likely country to succumb to such a strategy, which is an attempt to match strength against strength in an epic, mano-a-mano battle where China holds advantages in distance and mass that we are unlikely to ever overcome conventionally. If the Air Force is going to do its part in deterring the PRC, we must contribute to a viable offset strategy that relies as much on geography as technology. This is not to say that the PRC cannot effectively be fought, only that we cannot do so with a replay of techniques that proved successful over two decades ago over Iraq. It is to say that we are turning to the wrong war for our example. The war we should be basing our upon strategy is another conflict in which we fought an island nation that had successfully executed an “A2AD” strategy by physically occupying much of the Asian landmass from Manchuria to Burma to Wake and the Solomons. The example we are looking for, and should be planning to, is the Pacific War from 1941 to 1945. An analysis of the flow of goods and materials into and out of China reveals that with 98% of all freight moving by sea, China is practically, if not geographically, an island nation. As such, it is vulnerable to interdiction of trade routes to a far greater degree than a land power, and this is a national vulnerability that airpower is well-positioned to exploit – if applied properly. Background The Pacific War against Japan was not a quick war. Excepting the very end, it had no “shock and awe” component. It was a grinding advance across limited real estate to approach the Japanese home islands from the south while maintaining pressure on other fronts, including the interior of China, New Guinea and the Philippines, India and Burma. Fundamentally, it was a series of campaigns focused on establishing a logistical chain for Allied forces that would allow the application of airpower against Japan until such time as a massive amphibious assault could be undertaken or the home islands could be starved into submission. Equally important, it was a sustained counter-logistics campaign conducted against an island nation occupying island territory across the theater. The US executed a sustained maritime interdiction campaign beginning at the outset of the war. Admittedly, it was the only option available to the US Navy, but also one that had received a great deal of thought prior to the outbreak of war. The submarine war against Japan began immediately after the attack on Pearl Harbor – Admiral Hart, commander of the Asiatic Fleet, authorized unrestricted submarine warfare before the Japanese second wave had recovered aboard their carriers.[ii] While airpower accounted for more warships, submarines and mine warfare accounted for the majority of the Japanese merchant marine, sinking 1360 of the 2,117 large merchant ships sunk by US forces.[1] Despite the fact that Japan impressed captured ships into service, their merchant marine shrunk continuously during the war because of relentless Allied attack. Eventually, the Japanese merchant fleet was unable to perform its most basic functions; it could not replenish forward naval forces, move resources to Japan, supply outposts, or evacuate forces that could not be resupplied. The maritime interdiction campaign was essentially Joint a campaign intended to gain effects in what we would characterize today as an A2AD environment. Land-based air was the major source of airpower in the west, while carrier-based air supported successive island-hopping campaigns beginning in November 1943. Fifth Air Force’s (5AF) first responsibility was to gain control of the air, which entailed substantive offensive and defensive components with limited fighter resources. In 1942, 5AF bombers spent the majority of their time conducting logistics and counter-logistics, attacking Japanese maritime traffic, ports, airfields, and oil refineries. In their efforts to prevent the Japanese from reinforcing their forces in New Guinea, 5AF routinely attacked anything that moved on the water. While merchant ships loss statistics tell some of the story, they do not tell all of it. The official statistics only count ships of 500 tons displacement or greater used for long-haul routes. Short haul supply was supplemented by small watercraft of less than 500 tons displacement, commonly referred to as “barges”. 5AF in particular attacked watercraft during the day, from locally-built barges to tramp steamers and small warships, sinking them quite literally in the hundreds. In sea areas beyond the routine reach of aircraft and in joint attack areas by night, the naval interdiction effort was undertaken by PT Boats and submarines, ensuring constant pressure. By November 1942, Japanese Naval Forces in and around the Solomons ceased all offensive operations and light forces were dedicated almost entirely to resupply. By May of 1943, the Imperial Japanese Navy’s defensive perimeter did not enclose New Guinea, which was abandoned.[iii] Japanese deaths on New Guinea alone exceeded 148,000, the vast majority through disease and starvation.[iv] From November 1942 until the end of the war, 5AF claimed to have sunk 1.75 million tons of enemy shipping, excluding barges and similar small craft.[v] In the home islands, the effects of maritime interdiction were substantial. In 1941, Japan’s economic development was a fairly recent event. Japan began orienting the economy towards war in 1928, multiplying its heavy industrial production by 500% by 1940. The primary limitation on Japanese industry was the import of raw materials, including and especially oil, ferro-alloys, and nonferrous metals. They established strategic reserves in bauxite and oil.[vi] But attacks on shipping reduced the Japanese industrial base far below capacity. The economy was designed for a short, sharp war at the end of which the Japanese economy would have retained access to resources. Japan’s economy not structured or resourced for a long war against an industrial power. By 1943, oil was being successfully interdicted in part, and the flow of oil from the Dutch East Indies completely halted in April 1945. It is the opinion of the Survey that by August 1945, even without direct air attack on her cities and industries, the over-all level of Japanese war production would have declined below the peak levels of 1944 by 40 to 50 percent solely as a result of the interdiction of overseas imports… Even though the urban area attacks and attacks on specific industrial plants contributed a substantial percentage to the over-all decline in Japan’s economy, in many segments of that economy their effects were duplicative. Most of the oil refineries were out of oil, the alumina plants out of bauxite, the steel mills lacking in ore and coke, and the munitions plants low in steel and aluminum. Japan’s economy was in large measure being destroyed twice over, once by cutting off of imports, and secondly by air attack.[vii] The successful interdiction of the Indies did not completely shut off the flow of materials to Japan. Manchuria provided iron, coking coal (for steel), salt, bauxite and arable land (for food production), but did not provide significant sources of petroleum. Taiwan, a Japanese territory since 1895, provided resources including petroleum, but not nearly in sufficient quantities for wartime Japan. Even the Japanese investment in synthetic fuel production was centered offshore in China and Manchuria, and by 1944 the Japanese had reached their peak production, with 15 plants producing 717,000 barrels of oil.[viii] Combined with domestic production in 1944 of 1.6 million barrels from Japanese home islands, essentially only 9% of the annual oil demand was not subject to maritime interdiction.[ix] Japanese oil inventories in thousands of barrels[x] Fiscal Year Crude Petroleum Refined Products Starting Inventories Consump-tion Imports Production Total Imports Production Total Crude Refined Total 1941 3,130 1,941 5,071 5,242 15,997 21,239 20,857 28,036 48,893 36,974 1942 8,146 1,690 9,836 2.378 16,674 19,052 12,346 25,883 38,229 41,790 1943 9,848 1,814 11,662 4,652 16,167 20,819 6,839 18,488 25,327 43,992 1944 1,641 1,585 3,226 3,334 9,615 12,949 2,354 11,462 13,816 25,045 1945 (first half) 0 809 809 0 1,933 1,933 195 4,751 4,946 ~6,576 For the majority of the war, the short water route across from Korea to Japan was not interdicted. The Sea of Japan had proven a particularly difficult operating area for submarines, and it was not within reach of US aircraft. After USS Wahoo was declared lost in November of 1943, no US sub re-entered the Sea of Japan until June of 1945. But in March of 1945, Tinian-based B-29s began the largest aerial mining effort in history, codenamed operation STARVATION. The operation was intended to close the Shimonoseki Strait (also called the Kanmon Straits), blockade Tokyo and Nagoya in the adjacent inland sea, and mine ports in Korea and the northern Japanese coast. At the time, the Straits were the key maritime chokepoint, with 80% of Japan’s maritime traffic passing through.[xi] Total monthly traffic consisted of 1.25 million tons of shipping, consisting of 20-30 ships above 500 tons and 100-200 ships below 500 tons.[xii] STARVATION effectively shut down maritime traffic in targeted areas, accounting for more ships damaged or sunk during the last six months of the war than all other sources over the entire Pacific Theater combined.[xiii] The efforts to deprive Japan of needed resources were long-running and widespread. The mix of submarines, carrier aviation, and land-based airpower was an effective combination for conducting an extensive campaign at long ranges in spite of enemy defenses and a lack of local basing for Allied airpower. Despite plans for an invasion of the Japanese home islands, many senior airmen felt that Japan could be driven to surrender by a combination of maritime blockade and strategic bombing.[xiv] In any event, the use of Atomic weapons forced a rapid surrender and ended the debate. Nevertheless, it is clear that absent any direct attack on the home islands by any means, the maritime interdiction campaign had successfully brought Japan to the brink of surrender. Like any island nation, Japan was uniquely vulnerable to the interruption of sea traffic. China: The Island Nation We do not think of China as an island nation. After all, it has almost double the land border of the United States – 11958 nm – and borders 13 independent countries. But the land transportation links over these borders are extremely limited. The border terrain is unfavorable, dominated by desert, steppes, mountains (including the Himalayas) and jungle. Border disputes with several countries, including Bhutan, India and Pakistan, have delayed or prevented development of transportation infrastructure along the PRC borders. The total number of border “ports” along the Chinese Border stands at 90, counting the newest connection to the Afghanistan border but excluding airports. The capacity compares unfavorably with the 119 border crossings between the US and Canada alone.[xv] The comparison is inherently unbalanced, in that the Chinese border is relatively undeveloped, while the US-Canadian border has benefitted from more than two centuries of continuous expansion. The US and Canadian road and rail networks are effectively linked, whereas Chinese railroads do not even share the same gauge (track width) as any of their neighbors excepting Mongolia and North Korea, and sometimes not even then. Continuous rail lines extend only into Russia, Kazakhstan, North Korea or Vietnam, requiring either bogie exchange or cargo crossloading wherever there is a gauge change.[2] The total cross-border cargo carried by rail in 2012 was 54.24 million tonnes, with another 64.9 million tonnes[3] moved by truck.[xvi] This is a fraction of comparable US overland trade in that same year, where the rail systems moved 139 million tonnes with trucks moving 177 million tonnes.[xvii] Roughly a fifth (19 million tonnes in 2012[xviii]) of the PRC’s import flow by rail is coal mined in Mongolia. There are only five long-haul rail lines crossing the border at all, three crossing from Siberia and two from Kazakhstan, and those lines carry more exports than imports. The primary reason for the expansion of the PRC’s rail crossings in the last five years has been to carry exports to markets rather than to import goods or resources. The fifth line, Hunchun, has been closed for most of the last 15 years, but reopened in late 2013 and in 2014 moved comparatively little rail traffic, mostly coal. While the border crossings have been expanded and upgraded in the last five years, they are limited in capacity by the infrastructure on both sides of the border. All five lines are much more limited than their US counterparts, because they tend not to be double tracked (less than half of China’s rail lines are double-tracked)[xix] and do not have the high height limits of US trains, which can double-stack containers. The comparable road systems are also substantially less developed, with long distances between markets and much more limited capacity than the US interstate system. Also unlike the US, China’s international land ports are concentrated in five locations, all rail and road-served. Figure 1: China’s Border Port and National Railway Structure[xx] Port Country 2012 traffic (metric tonnes) Horgos Kazakhstan 22,000,000[xxi] Dostyk Kazakhstan 15,000,000[xxii] Hunchun Russia 0 (600,000 in 2014)[xxiii] Manzhouli Russia 30,060,000[xxiv] Suifenhe Russia 8,000,000[xxv] Table 1: 2012 Traffic through the five major PRC border ports with rail freight Table 2 shows the total cross-border cargo movement traffic for 2012, which includes river, road and rail traffic. Air traffic and petroleum pipelines are not included. Notably, there were no exploitable land routes to Afghanistan (even now, the road only goes to the PRC side of the border) or Bhutan, which does not even have diplomatic relations with China. Despite the fact that China is India’s largest trading partner, the countries do not exchange goods across their disputed border. Country Ports Number Foreign trade cargo (1000 tonnes) Percent (%) Kazakhstan 9 40,884 33.6 Mongolia 13 34,851 28.6 Russia 23 31,783 26.1 Vietnam 10 4655 3.8 Burma 5 3621 3.0 North Korea 15 3513 2.9 Kyrgyzstan 2 1048 0.9 Laos 4 1005 0.8 Tajikistan 1 173 0.1 Nepal 4 174 0.1 Pakistan 1 59 0.0 Afghanistan 0 0 0.0 Bhutan 0 0 0.0 India 0 0 0.0 TOTAL 87 121,766 Table 2: Overland foreign trade cargo in 2012[xxvi] China has three international oil pipelines, crossing from Russia, Kazakhstan and Burma. The total capacity is advertised as 980,000 barrels per day, but this number is deceptive. The largest capacity pipeline, through Burma, has yet to move more than test quantities of oil, although it has been moving natural gas. The Sino-Burmese oil pipeline is limited by the fact that while the pipeline exists, the oil has nowhere to go once it reached the Chinese terminus in Kunming. The refinery that was supposed to be built in Kunming hasn’t broken ground as of this writing and there are no internal oil pipelines from Kunming to elsewhere in China. The Energy Sector[4] China is not entirely self-sufficient in any of the non-renewable energy sources that it uses to provide electricity and transportation. As a result, China has two key vulnerabilities on the energy front. The first is the distribution network within country, which is highly energy-intensive, and largely dependent on oil. This ties together with electricity generation, in that China’s power generation capacity is mostly coal-dependent, and coal is dependent on surface transport for distribution. For 2013, coal provided 65% of China’s energy consumption, which has been a relatively constant figure for the last decade.[xxvii] China meets 96% of its coal demand domestically, meaning that effective coal interdiction would have to be accomplished by affecting the domestic transportation network. Chinese coal imports tend towards coking coal for industrial processes, versus steam coal for power generation. Figure 2: China’s Energy Infrastructure. Crude oil pipelines are in green (orange if international), and oil product pipelines are blue. Refineries (gas pumps) that produce jet fuel are red, with orange producing jet fuel components. Green refineries mostly produce chemicals and no fuel. Oil terminals are green ships, green and purple circles are the SPR sites, and the rail network is in red. No teakettle refineries or province borders are displayed. The second vulnerability is that the PRC imports the majority of its petroleum, and the maritime petroleum transport network involves long distance movement that the PRC cannot possibly protect. As of 2014, China is the world’s second largest oil importer, approaching the US. Throughout 2014, China averaged 6.2 million barrels per day (bpd), compared to 7.4 million bpd for the US. However, in February 2015, China’s oil imports spiked at an average rate of 7.53 million bpd, exceeding the US for the month. Driven in part by low oil prices, China is assessed to be filling strategic reserves while prices are low, maintaining at least a 30-day supply of imported oil (and probably closer to 100 days).[xxviii] As with coal, China’s demand exceeds domestic production, but China imports much more oil, approaching 60% of its total requirement. Petroleum import data alone gives an incomplete picture of China’s fuel requirements. Crude oil is simply sticky black goo with very little utility in its unrefined state. Refining is necessary to turn that goo into useable fuels. In 2013, China’s total refining capacity was 12.6 million bpd, behind only the US at 17.8 million bpd and representing a comfortable overcapacity of about 24%.[xxix] The output of China’s refineries has typically focused on lighter distillates, tending towards diesel fuel and gasoline, which allowed China to become a net diesel fuel exporter in 2012. In 2014, driven by a strong market, Chinese major refineries switched to the more profitable middle distillates (naphtha, kerosene and jet fuel), becoming a net jet fuel/kerosene exporter and reversing a trend that had seen China as Asia’s largest jet fuel importer only a year earlier.[xxx] This occurred despite the fact that China’s smaller, private “teakettle” refineries, which account for a quarter of the nation’s refinery capacity, produce no jet fuel components at all.[xxxi] Overall, China’s expansion of its refinery capability within the past four years has left the PRC able to meet 98% of its demand for petroleum distillates, and capable of having a net export balance for all distillate fuels except naphtha.[xxxii] China’s vulnerability to supply interdiction is largely limited to crude oil, although as naphtha is a key ingredient for jet fuel, this remaining import dependency is still significant. Maritime Dependency By comparison to trade across land borders, China’s sea trade is massive. Using figures from only the top 15 coastal ports, the volume of seaborne trade in 2013 came to 7.28 billion tonnes, up from 6.65 billion tonnes in 2012[xxxiii]. Using 2012 figures, this means that international road and rail trade comes to less than 1.8% of the volume of freight transported by sea; that disparity is likely to have increased in 2013 and 2014 as the amount of seaborne trade is increasing at a faster rate than any other transport mode in both relative and absolute terms. Put another way, the annual movement of freight through all of China’s international borders is matched in under 60 days by Shanghai’s port complex alone.[xxxiv] There is no conceivable condition under which China’s land trade routes could mitigate a maritime interdiction campaign. Figure 3: China’s Crude Oil Imports By Source (2013) (USEIA) The huge disparity between land and sea trade is likely to continue to increase. Overland trade is infrastructure-limited, and depends heavily on road and rail infrastructure in neighboring countries. Russia’s pipeline and rail infrastructure in Siberia has to serve multiple customers, including Russia itself, Japan, and Korea. With sea trade essentially a global phenomenon, the infrastructure is well-established and continuing to expand worldwide, without intermediate bottlenecks. For China, this means that this trade flow is subject to interdiction. China’s power projection capability is limited, and the maritime geography is strategically unfavorable. The first and second island chains hem in China, putting it in a position where all of its maritime trade must pass through waterways that can be controlled (or at least denied) by foreign powers. China’s maritime trade generally passes through a number of chokepoints, most especially the Straits of Malacca. Overland transport of oil via pipeline and rail accounts for less than 10% of all oil imports, and this only from Russia and Kazakhstan. Even Russia relies on maritime transport for oil; in 2014, 55% of the oil imported from Russia went by sea rather than pipeline or rail.[xxxv] Looking at the rest of the totals, it’s clear that around 85% of the oil imported into China passes through the Straits of Malacca (77%) or the Panama Canal (8%). Around fifty percent of the PRC’s oil imports pass through two chokepoints rather than just one – the Straits of Hormuz, the Panama Canal or Bab al Mandar as well as Malacca. The limits on the Straits of Malacca have a real impact on ship design, as ships too long or deep for the narrow passageway have to detour around Indonesia and sail through the Lombok Strait. Tanker sizes have actually shrunk since the 1970s partly because of this; “Malaccamax” designs are the largest ships able to transit the Straits of Malacca, and are classed a Very Large Crude Carriers (VLCCs). A typical VLCC can carry two million barrels of oil, but is reliant on offshore terminals or smaller tankers for loading and offloading. A single VLCC carries about four days maximum flow for the Siberian and Kazakh pipelines combined. Eleven to fifteen of these vessels pass through Malacca daily, in both directions. Figure 4: Maritime Freight Traffic 3rd Semester 2013 (Marinetraffic.com) From a military standpoint, the majority of maritime trade is irrelevant. Container ships, which are used to move commercial goods, constitute the majority of the maritime traffic and are not militarily relevant except for spare parts and system components. Similarly, while China imports vast quantities of raw materials (particularly iron), domestic production of most raw materials such as metal ores, minerals, rare earths and potash is among the top three global producers, depending on the year.[xxxvi] In the 1930s, Japanese military expansion looked towards China’s resources as a solution to Japan’s natural resource shortages, recognizing that China is comparatively resource-rich. While China cannot fuel its industrial machine with domestic products alone, it has the capacity to maintain its military industry almost entirely with domestic supplies of raw materials. China’s vulnerability is related to the fact that while its resources are large, the country’s massive consumption exceeds the capability of domestic resource production. Nowhere is this more apparent than in the energy sector, where Chinese demand for coal, petroleum and natural gas is satiated only through foreign imports. Indeed, it is these energy imports that could provide a key degree of leverage on the military front. The energy supply from overseas powers all of China’s power projection capabilities, along with the industries that produce it and the transportation network that supplies and moves it. Implications The vast majority of seaborne imports come from well outside the capability of the PLAAF or PLAN to effectively protect. Unlike Japan and South Korea, which could reasonably expect to maintain northern supply routes to Alaska against Chinese opposition, the Chinese have no such geographical advantage or supporting alliance structure. Moreover, in any conflict with China, the US would start in a much more favorable position than it did against Japan in 1941. We have more combat power forward, our partners are nations in their own right and not poorly defended colonial outposts, and this time we are not opposing a Japan that has already expanded. China today cannot yet compare with Imperial Japan for amphibious sealift and will not have a decade-long running start on territorial expansion on the Asian Mainland. Certainly, our forward basing posture leaves US forces subject to direct attack from the PRC proper, but the islands which host our facilities are not under the threat of occupation. The unfavorable maritime geography and dependency on overseas trade leaves China vulnerable to a Strategic Interdiction strategy – a Joint effort designed to prevent the movement of resources related to military forces or operations. While a deeper discussion of Strategic Interdiction is a subject for a follow-on paper, an overview of such a strategy can be outlined and applied to China. In contrast with maritime interdiction, Strategic Interdiction (SI) is not a broad blockade but is a targeted effort to interdict primarily the production and transport of energy resources. A campaign would have four elements: A “Counterforce” effort designed to attrit the adversary air forces (particularly bombers), naval forces (gray hulls) and naval auxiliaries (replenishment) to the point where they can neither project military power nor defend against US power projection, at least far beyond the PRC continental shelf.[5] An “Inshore” element, which consists of operations to deny effective use of home waters, including rivers and coastal waters. Standoff or covert aerial mining is a key component of this element. An “Infrastructure Degradation” plan intended to disrupt or destroy specific soft targets, such as oil terminals, oil refineries, pipelines and railway chokepoints such as tunnels and bridges. Many of these targets would be in airspace not defended by ground-based air defense. A “Distant” maritime strategy, which occurs out of effective adversary military reach, intended to interdict energy supplies. This strategy is aimed primarily at bulk petroleum carriers (tankers) and secondarily at coal transports, and not at container, dry bulk, or passenger vessels. Such a strategy might not be lethally oriented, directed instead towards the seizure and internment of PRC-bound vessels. A strategic interdiction campaign is fundamentally a logistically based strategy. The primary objective is to effectively neutralize certain elements of PRC military power by starving them of energy. In effect, this strategy targets naval and air forces, which rely on jet fuel, and leaves the gasoline and diesel-dependent army to compete with domestic fuel needs – because without the PLAAF and the PLAN, the PLA doesn’t ever leave the mainland. The primary targets are air and naval forces, but they are affected by an indirect route that is difficult to counter over the medium to long term. Much has been said, with respect to PRC missile forces, that the objective is to “shoot the archer”, the implication being that such an action would prevent the archer from launching standoff weapons against air or surface targets. An SI campaign is designed to starve the archer, the guys who protect the archer, the folks who make, carry and deliver the arrows, and the people who brought the archer to the battlefield in the first place. A complete campaign design would take advantage of the relationship between energy and infrastructure to disrupt a slice of the energy web in as many places as possible. Such a strategy is inherently asymmetric for the US, in that it cannot succeed against our mainland. Our maritime geography is extremely favorable, with four coasts that are difficult to interdict, two of which are not adjacent to the Pacific. The power projection capability required to conduct a maritime interdiction campaign against the US is well outside any projected PLAN capability. The strategy also takes advantage of the US advantage on blue-water naval capabilities and long-range strike aircraft. Indeed, the US airpower advantage is critical to any interdiction campaign, just as it was in World War II. Wrapup Against the USSR, the United States elected not to undertake an approach that was intended to directly offset the Soviet advantage in numbers and the vulnerabilities of Europe to a ground invasion. Instead, it adopted offset strategies to asymmetrically counter the USSR’s strengths, leading to both tactical nuclear weapons and a revolution in precision munitions and sensors. A quarter century after the fall of the wall, it is perhaps time to adopt a third offset strategy aimed squarely at the PRC. For more than two decades, the standing USAF template for applying combat airpower against a target country has been the DESERT STORM model. While this model may still have some applicability, it is long past time to abandon it for a conflict against a peer or near-peer nation. DESERT STORM was conducted against an adversary that was surrounded by enemies, outnumbered, technologically outmatched, and attacked by a force that had unlimited local basing, was better trained, better led, and better equipped. None of those conditions will apply in a conflict with China, where we are likely to have parity in a number of these areas, a slight degree of superiority in others, and a critical disadvantage in basing, numbers, and magazine depth. It makes no sense to attempt to enter a fight on Chinese terms, in their own front yard, against a massive opponent who has historically demonstrated the ability to take a great number of punches on home ground and still stay in the fight.

### 2NC---Prevents Escalation

#### Provocative friction is good --- reduces escalation by demonstrating capability, and the capacity to escalate deters attackers from crossing red lines --- the aff undermines both dynamics

Jon **Lindsay and** Erik **Gartzke 14**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies, AND Erik Gartzke is Professor and Director of cPASS at the Department of Political Science @ UCSD, Lindsay, Jon R., and Erik Gartzke. “Coercion through Cyberspace: The Stability-Instability Paradox Revisited.” The Power to Hurt: Coercion in the Modern World, Oct. 2014.

1 Introduction Information technology is the nervous system of the global economy. Critical infrastructure for banking, power, transportation, and industry increasingly depends on embedded computers connected to the internet. Firms and citizens entrust vital personal, medical, and financial data to distant servers in return for more convenient and efficient services. Military command and control relies on digital networks to connect far-flung surveillance and strike systems and to project power rapidly and precisely. Yet this vital interconnectivity also facilitates new modes of crime, protest, espionage, and warfare. Ubiquitous computer networks both provide access to valuable targets and become targets themselves. Protecting and influencing cyber infrastructure has thus become a major priority for governments and other political actors around the world. The very ubiquity of information technology makes the danger of cyber threats easy to exaggerate. In contemporary defense policy discourse there are three influential narratives of mounting cyber peril. The most dangerous envisions the paralysis of industrial control systems of military command and control through surprise attack by anonymous hackers. This scenario is often described as a “digital Pearl Harbor” or a “cyber 9/11” depending on whether the imagined aggressor is a revisionist state like China or Iran or a non-state anarchist or terrorist empowered by the information revolution. A second narrative offers an alternative to the shock of sudden catastrophe by warning of the long term erosion of economic and military competitiveness. The relentless theft of vital secrets stored on corporate and government networks is thus thought to cause a prolonged “death by a thousand cuts.” In both of these scenarios, weaker states and terrorists gain increasing access to powerful hacking tools while technology-dependent advanced industrial states become increasingly vulnerable to cyber attack and exploitation. 1 A third category of threat narrative concerns the transformation of internet architecture to decisively benefit one political group at the expense of the other. At one extreme, the growth of flexible social media enables connected protesters to overwhelm and overthrow authoritarian regimes.2 At the other extreme governments censor and reconfigure the internet to undermine innovation and freedom. State paranoia about paralysis and erosion thus leads to digital lockout or “the end of the internet” as we know it.3 National security officials, the defense industry, and media pundits all have incentives to exaggerate the cyber threat.4 The secrecy of cyber operations further complicates assessment, even as states make major investments in cyber defense. Each of the three narratives above are indeed exaggerations, but they point toward more plausible scenarios using cyber operations as subtle complements to or even substitutes for more traditional forms of aggression. Understanding the dynamics, magnitude, and likelihood of aggression online requires greater attention to the operational requirements for staging various types of cyber operations, the strategic benefits actors hope to gain through them, and the risks of unintended consequences. Too often defenders of the cyber revolution focus narrowly on the technological possibility for harm but discount operational and institutional obstacles to effectiveness and ignore the strategic utility of cyber harm or threats of harm. 5 A realistic appraisal of cyber threats must take not only technological but also strategic logic into account. Thomas Schelling distinguishes brute force, which is needed in a contest of strength, from coercive threats, which are useful in a contest of resolve.6 Both require the power to inflict harm, but brute force exercises it while coercion holds (at least some of) it in reserve. Likewise, actors might use cyber operations to attempt to change the balance of power directly or they might use them to provide information about their intentions and commitment. To paraphrase Clausewitz, cyberwar is politics by other means. As a result of technical and political constraints, the coercive potential of cyberspace is more limited than generally appreciated, but it is not negligible, especially when exploited in conjunction with other forms power such as military force. In this chapter we lay out a typology of cyber operations, distinguishing the skills and resources needed to cause different types of harm. Not all cyber options are equally available to all actors because of varying requirements in organizational capacity, intelligence support, and risk sensitivity. For each of the exaggerated myths mentioned above, there are low-cost, low- payoff irritants widely available as well as higher-cost, potentially higher-payoff adjunct capabilities available to a more restricted set of predominantly nation-state actors. Next we evaluate the coercive utility of these various harms, or threats of these harms, by taking into consideration the interaction of cyberspace with other domains. Finally we ask, what types of cyber coercion are most likely? We argue that there exist two important bounds on the distribution of cyber harm. First, because voluntary connections to the internet make cyber harms possible in the first place, aggressors must be careful not to provoke their victims to disconnect. Second, the availability of military instruments beyond the cyber domain, creates potential for retaliation for unacceptable harms. These constraints combine to make small-scale cyber aggression relatively appealing and thus more likely while making large-scale aggression difficult and undesirable for initiators and thus less likely. The finding of this chapter extends the logic of the stability-instability paradox pioneered in the 1960s. While nuclear weapons can deter nuclear war, they can fail to deter, and even encourage, conventional or peripheral war. Mutually assured destruction restrained the superpowers from engaging in direct confrontations during the Cold War, even as this restraint encouraged and facilitated the exercise of proxy wars throughout the Third World. The mechanisms of restraint in the cyber domain are slightly different than in the nuclear world—the risk of voluntary disconnection and military retaliation vs. mutual Armageddon—but the results are similar: little truly dangerous behavior and a lot of provocative friction. The social and economic value of the internet expands the scope for minor aggression like espionage, covert influence, and symbolic protest. Cyber operations also act as valuable adjuncts for battlefield operations akin to signals intelligence and electronic warfare for states who are willing and able to go to war for other reasons. However, there are diminishing incentives to “go big” with cyber warfare alone given the incentives targets have to identify even a hard-to-identify attacker and shift domains to punish cyber aggression. Although the attribution of the attacker’s identity is widely thought to be hard problem in cyberspace, anonymity is never guaranteed and might not even be useful for some forms of coercion. A nonzero risk of attribution opens the door to retaliatory punishment, which encourages attackers to exercise restraint in cyber aggression. Ironically enough, the instability we perceive in cyberspace is indicative of the stability of deterrence of the most dangerous cyber threats.

#### Cold war empirics prove --- tactical instability creates strategic calm

Jon **Lindsay 15**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies., Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security, vol. 39, no. 3, Jan. 2015, pp. 7–47.

Barring gross misperception, however, one can expect the risk of unwanted escalation from cyber to other military domains to deter both sides from resorting to more destructive forms of computer network attack in most situations. 113 Yet although nuclear or conventional deterrence might be able to check catastrophic cyberattack, it cannot credibly discourage minor cyber aggression such as nationalist hacktivism, industrial espionage, or harassment of dissident expatriates. Indeed, the observable pattern of Chinese (and American) cyber activity conforms to the logic of the Cold War stability-instability paradox, but in slightly revised form. In the original formulation of the paradox, mutual vulnerability to nuclear retaliation inhibits nuclear war but encourages conventional war in peripheral theaters where nuclear threats are not credible.114 Today, the intensity of cyber aggression is bounded by the risk of any form of military retaliation as well as the need to preserve interconnection and protect sources and methods that rely on deception. Cyberattackers intentionally keep the costs they inflict below the assessed threshold of even limited military retaliation by opponents, occupying a region where military threats of punishment would be utterly noncredible. The aggressor’s freedom of action is further constrained by the need to maintain stealth and plausible deniability for ongoing operations. Actors that are deterred by threats of military punishment, on the one hand, and threats of counterintelligence detection or loss of connection, on the other, are encouraged to find more limited ways to inflict costs. The complexity of modern computer network infrastructure, in particular, offers many inexpensive ways to inflict minor costs. One implication is that cyberspace creates more scope for nontraditional security concerns (e.g., harassment of human rights organizations and vulnerable user communities) that powerful actors usually ignore in their focus on protecting high-value economic and military assets.115 As long as dense interconnection and economic interdependence remain mutually beneficial for powers such as the United States and China, they will be able to tolerate the irritants that they will inevitably inflict on one another. The modern intelligence-counterintelligence contest plays out in a complicated sociotechnical space where states take advantage of economic cooperation and hedge against security competition. If their broader mutual interest frays, however, then cyberwarfare becomes just one facet of a more serious strategic problem involving more dangerous means. Exaggeration of the cyber threat feeds spirals of mistrust, which make this undesirable outcome slightly more likely. The United States and China should discuss the interaction of cybersecurity and traditional military force in depth and take steps to limit misunderstandings about the other’s intentions. They might even learn to interpret chronic cyber friction as a sign that more truly dangerous threats have been constrained. Contrary to conventional wisdom, the emergence of complex cyber threats may be a positive development in the tragic history of international politics: the bad news about cybersecurity is good news for global security.

#### Cyberwar reduces physical war

Thomas **Rid 13**, THOMAS RID is a Reader in War Studies at King’s College London, 12-1-2013, "Cyberwar and Peace," Foreign Affairs, https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace

Cyberwar Is Coming!” declared the title of a seminal 1993 article by the RAND Corporation analysts John Arquilla and David Ronfeldt, who argued that the nascent Internet would fundamentally transform warfare. The idea seemed fanciful at the time, and it took more than a decade for members of the U.S. national security establishment to catch on. But once they did, a chorus of voices resounded in the mass media, proclaiming the dawn of the era of cyberwar and warning of its terrifying potential. In February 2011, then CIA Director Leon Panetta warned Congress that “the next Pearl Harbor could very well be a cyberattack.” And in late 2012, Mike McConnell, who had served as director of national intelligence under President George W. Bush, warned darkly that the United States could not “wait for the cyber equivalent of the collapse of the World Trade Centers.” Yet the hype about everything “cyber” has obscured three basic truths: cyberwar has never happened in the past, it is not occurring in the present, and it is highly unlikely that it will disturb the future. Indeed, rather than heralding a new era of violent conflict, so far the cyber-era has been defined by the opposite trend: a computer-enabled assault on political violence. Cyberattacks diminish rather than accentuate political violence by making it easier for states, groups, and individuals to engage in two kinds of aggression that do not rise to the level of war: sabotage and espionage. Weaponized computer code and computer-based sabotage operations make it possible to carry out highly targeted attacks on an adversary’s technical systems without directly and physically harming human operators and managers. Computer-assisted attacks make it possible to steal data without placing operatives in dangerous environments, thus reducing the level of personal and political risk. These developments represent important changes in the nature of political violence, but they also highlight limitations inherent in cyberweapons that greatly curtail the utility of cyberattacks. Those limitations seem to make it difficult to use cyberweapons for anything other than one-off, hard-to-repeat sabotage operations of questionable strategic value that might even prove counterproductive. And cyber-espionage often requires improving traditional spycraft techniques and relying even more heavily on human intelligence. Taken together, these factors call into question the very idea that computer-assisted attacks will usher in a profoundly new era. THE THIN CASE FOR CYBERWAR One reason discussions about cyberwar have become disconnected from reality is that many commentators fail to grapple with a basic question: What counts as warfare? Carl von Clausewitz, the nineteenth-century Prussian military theorist, still offers the most concise answer to that question. Clausewitz identified three main criteria that any aggressive or defensive action must meet in order to qualify as an act of war. First, and most simply, all acts of war are violent or potentially violent. Second, an act of war is always instrumental: physical violence or the threat of force is a means to compel the enemy to accept the attacker’s will. Finally, to qualify as an act of war, an attack must have some kind of political goal or intention. For that reason, acts of war must be attributable to one side at some point during a confrontation. No known cyberattack has met all three of those criteria; indeed, very few have met even one. Consider three incidents that today’s Cassandras frequently point to as evidence that warfare has entered a new era. The first of these, a massive pipeline explosion in the Soviet Union in June 1982, would count as the most violent cyberattack to date -- if it actually happened. According to a 2004 book by Thomas Reed, who was serving as a staffer on the U.S. National Security Council at the time of the alleged incident, a covert U.S. operation used rigged software to engineer a massive explosion in the Urengoy-Surgut-Chelyabinsk pipeline, which connected Siberian natural gas fields to Europe. Reed claims that the CIA managed to insert malicious code into the software that controlled the pipeline’s pumps and valves. The rigged valves supposedly resulted in an explosion that, according to Reed, the U.S. Air Force rated at three kilotons, equivalent to the force of a small nuclear device. But aside from Reed’s account, there is hardly any evidence to prove that any such thing happened, and plenty of reasons to doubt that it did. After Reed published his book, Vasily Pchelintsev, who was reportedly the KGB head of the region when the explosion was supposed to have taken place, denied the story. He surmised that Reed might have been referring to a harmless explosion that happened not in June but on a warm April day that year, caused by pipes shifting in the thawing ground of the tundra. Moreover, no Soviet media reports from 1982 confirm that Reed’s explosion took place, although the Soviet media regularly reported on accidents and pipeline explosions at the time. What’s more, given the technologies available to the United States at that time, it would have been very difficult to hide malicious software of the kind Reed describes from its Soviet users. Another incident often related by promoters of the concept of cyberwar occurred in Estonia in 2007. After Estonian authorities decided to move a Soviet-era memorial to Russian soldiers who died in World War II from the center of Tallinn to the city’s outskirts, outraged Russian-speaking Estonians launched violent riots that threatened to paralyze the city. The riots were accompanied by cyber-assaults, which began as crude disruptions but became more sophisticated after a few days, culminating in a “denial of service” attack. Hackers hijacked up to 85,000 computers and used them to overwhelm 58 Estonian websites, including that of the country’s largest bank, which the attacks rendered useless for a few hours. Estonia’s defense minister and the country’s top diplomat pointed their fingers at the Kremlin, but they were unable to muster any evidence. For its part, the Russian government denied any involvement. In the wake of the incident, Estonia’s prime minister, Andrus Ansip, likened the attack to an act of war. “What’s the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?” he asked. It was a rhetorical question, but the answer is important: unlike a naval blockade, the disruption of websites is not violent -- indeed, not even potentially violent. The choice of targets also seemed unconnected to the presumed tactical objective of forcing the government to reverse its decision on the memorial. And unlike a naval blockade, the attacks remained anonymous, without political backing, and thus unattributable. A year later, a third major event entered the cyber-Cassandras’ repertoire. In August 2008, the Georgian army attacked separatists in the province of South Ossetia. Russia backed the separatists and responded militarily. The prior month, in what might have been the first time that an independent cyberattack was launched in coordination with a conventional military operation, unknown attackers had begun a campaign of cyber-sabotage, defacing prominent Georgian websites, including those of the country’s national bank and the Ministry of Foreign Affairs, and launching denial-of-service attacks against the websites of Georgia’s parliament, its largest commercial bank, and Georgian news outlets. The Georgian government blamed the Kremlin, just as the Estonians had done. But Russia again denied sponsoring the attacks, and a NATO investigation later found “no conclusive proof” of who had carried them out. The attack set off increasingly familiar alarm bells within American media and the U.S. national security establishment. “The July attack may have been a dress rehearsal for an all-out cyberwar,” an article in The New York Times declared. Richard Clarke, a former White House cybersecurity czar, warned that the worst was yet to come: the Georgian attack did not “begin to reveal what the Russian military and intelligence agencies could do if they were truly on the attack in cyberspace.” Yet the actual effects of these nonviolent events were quite mild. The main damage they caused was to the Georgian government’s ability to communicate internationally, thus preventing it from getting out its message at a critical moment. But even if the attackers intended this effect, it proved short-lived: within four days after military confrontations had begun in earnest, the Georgian Foreign Ministry had set up an account on Google’s blog-hosting service. This move helped the government keep open a channel to the public and the news media. What the Internet took away, the Internet returned. ISTOCK.COM / -ANTONIO- Overblown: keyboard as grenade. IN CODE WE TRUST? Perhaps the strongest evidence presented by advocates of the concept of cyberwar is the Stuxnet operation launched against Iran by the United States and Israel. Stuxnet, part of a set of attacks known as Operation Olympic Games, was a sophisticated multiyear campaign to sabotage Iran’s nuclear enrichment facility in Natanz by inserting a harmful computer worm into the software that ran the facility’s centrifuges, causing them to overload. American and Israeli developers started designing the project as early as 2005, and it launched in 2007, growing more sophisticated until its discovery in 2010. The attack was groundbreaking in several ways. The developers built highly target-specific intelligence into the code, enabling the Stuxnet software to make autonomous decisions in its target environment. Most important, Stuxnet represented the first and only physically destructive cyberattack launched by one state (or, in this case, two states) against another. Yet even cyberattacks that cause damage do so only indirectly. As an agent of violence, computer code faces a very basic limit: it does not have its own force or energy. Instead, any cyberattack with the goal of material destruction or harming human life must utilize the force or energy embedded in its target: for example, shutting down an air traffic control system and causing trains or planes to crash or disrupting a power plant and sparking an explosion. Yet besides Stuxnet, there is no proof that anyone has ever successfully launched a major attack of this sort. Lethal cyberattacks, while certainly possible, remain the stuff of fiction: none has ever killed or even injured a single human being. Thanks to its lack of direct physical impact, code-induced violence also has less emotional impact. It would be difficult for a cyberattack to produce the level of fear that coordinated campaigns of terrorism or conventional military operations produce. Owing to their invisibility, cyberweapons also lack the symbolic power of traditional ones. Displays of weaponry, such as the elaborate military parades put on by China and North Korea, sometimes represent nothing more than nationalist pageantry. But revealing one’s arsenal can also serve tactical and strategic ends, as when countries deploy aircraft carriers to demonstrate their readiness to use force or carry out operations designed to intimidate the enemy, such as using military aircraft to conduct deliberately low flyovers. Indeed, displaying weapons systems and threatening to use them can prove more cost-efficient than their actual use. But cyberweapons are hard to brandish. Perhaps the most crucial limitation of violence in cyberspace is its almost entirely destructive quality: unlike traditional political violence, which can maintain trust in institutions and states as well as undermine it, violence in cyberspace can do only the latter. Any established political order comes with a certain degree of inherent violence; consolidated states, after all, survive only if they maintain monopolies on the legitimate use of force. By encouraging trust in the ability of state institutions to protect property and safeguard citizens, this inherent violence buttresses a state’s power and allows the state to establish the rule of law. But cyber-violence lacks this ability, since it does little or nothing to build up trust in institutions; indeed, it is very difficult to imagine how cyberattacks could be used to enforce rules or laws, either domestically or internationally. Digital surveillance presents a more complicated picture. In democracies, intelligence agencies tread a thin line between providing security and eroding public trust in the state, as demonstrated by the recent controversy over the U.S. National Security Agency’s data-collection practices. In authoritarian countries, digital surveillance can assist the state’s coercive use of force, but it cannot replace it. Such limitations, however, should not lead anyone to dismiss the corrosive potential of cyberattacks. Indeed, such assaults can undermine social trust in a more direct way than traditional political violence. Cyberattacks are more precise; they do not necessarily undermine the state’s monopoly of force in a wholesale fashion. Instead, they can be tailored to attack specific companies or public-sector organizations and used to undermine those groups’ authority selectively. Stuxnet provides a good example of this dynamic. Putting aside the question of whether the attack was an act of war, its primary intention was to undermine the trust of the Iranian scientists in their systems and in themselves and the trust of the Iranian regime in its ability to build nuclear weapons. The original intention was to cause physical damage to as many Iranian centrifuges as possible. But the American and Israeli attackers knew that the physical effect could be exploited to unleash a much more damaging psychological effect. “The intent was that the failures should make them feel they were stupid, which is what happened,” an American participant told The New York Times. The Americans and the Israelis hoped that once a few machines failed, the Iranian engineers would shut down more machines because they distrusted their own technology or indeed their own skills. At the headquarters of the International Atomic Energy Agency, in Vienna, rumors circulated that the Iranians had lost so much confidence in their own systems and instruments that the management of the Natanz facility took the extraordinary step of assigning engineers to sit in the plant and radio back what they saw to confirm the instrument readings. “They overreacted,” one of the attackers revealed to David Sanger of The New York Times, “and that delayed them even more.” The Iranians also began to assign blame internally, pointing fingers at one another and even firing some personnel. DIGITAL UNDERGROUND Damaging though it may have been, Stuxnet, along with the cyber-scuffles in Estonia and Georgia, represents not a new form of warfare but something more akin to other, less lethal forms of aggression: sabotage and espionage. Unlike acts of war, these political crimes, which are often committed by nonstate actors, need not be violent to work. And although saboteurs and spies do act politically, they often seek to avoid attribution, unlike those who launch acts of war. For those reasons, the cyber-era has been a boon for political crime. Consider sabotage. Before the computer age, saboteurs had trouble calibrating and controlling the effects of their actions. Sabotage had to target physical property and relied on physical violence, which often proves unpredictable. During postal and railway strikes in France in 1909 and 1910, for instance, saboteurs cut signal wires and tore down telegraph posts. Destroying property risked running afoul of public opinion, and the tactic ultimately divided the workers. The strikes themselves, as a form of sabotage, also ran the risk of leading to unpredictable violence: indeed, labor demonstrations often intensified into riots, making it easier for opponents to portray the strikers as uncompromising radicals. It is much easier for saboteurs to avoid counterproductive side effects in the age of computer-assisted attacks, which can contain violence and generally avoid it altogether. Cyberattacks can maliciously affect software and business processes without interfering with physical industrial processes, remaining nonviolent but sometimes still causing greater damage than a traditional assault. A 2012 attack against the computer network of the oil company Saudi Aramco illustrates this potential. The attack physically harmed neither hardware nor humans. Yet by allegedly erasing the hard disks of some 30,000 computers, the attackers likely did much more monetary damage to Saudi Aramco than they could have through an act of traditional sabotage against machinery in one of the company’s plants. The oil giant reportedly had to hire six specialized computer security firms to help with its forensic investigation and post-attack cleanup. Despite such potential, it is also important to remember the inherent limitations of computer-assisted political crime and to note that human agents remain critical in the age of digital violence. Even Stuxnet, the most successful example of cyber-sabotage, demonstrates this fact. For the United States and Israel, the “holy grail,” in the words of one of the attack’s architects, was getting a piece of malicious software into the control system at Natanz. The Americans and Israelis needed fine-grained data from inside the Iranian plant to develop their weaponized code. The problem was that the control system was protected by an air gap: it was not connected to the Internet or even internal networks. As a result, the attackers had to deliver the malicious code via a removable hard drive such as a USB flash drive -- delivered by a human hand. To make this happen, U.S. intelligence operatives first obtained a list of the people who were visiting the targeted plant to work on its computer equipment and who could carry the payload there. “We had to find an unwitting person on the Iranian side of the house who could jump the gap,” one planner later told Sanger. The list of possible carriers included engineers from the German company Siemens, who were helping their Iranian colleagues maintain the control system -- work that required the Siemens engineers to bring portable computers into the plant. Precisely how the U.S.-Israeli team managed to exploit this vulnerability remains unknown. Suffice it to say that although “Siemens had no idea they were a carrier,” in the words of one U.S. official quoted by Sanger, “it turns out there is always an idiot around who doesn’t think much about the thumb drive in their hand.” SAFETY IN ONES AND ZEROS If cyberattacks reduce the amount of violence inherent in conflict, and if they often take the form of sabotage or espionage, then many officials and commentators who have been warning about the dawn of cyberwar have been ringing false alarms. Digital violence does have implications for ethics and for national security strategy, however. Weaponized code, or cyberattacks more generally, can achieve goals that used to require conventional force. The most sophisticated cyberattacks are highly targeted, and cyberweapons are unlikely to cause collateral damage in the same way conventional weapons do. Therefore, in many situations, the use of computers would be ethically preferable to the use of conventional weapons: a cyberattack might be less violent, less traumatizing, and more limited.

#### Cyber-warfare is good—it prevent kinetic conflict and keeps war cool

Arquilla 12 - John Arquilla earned his degrees in international relations from Rosary College (BA 1975) and Stanford University (MA 1989, PhD 1991). He has been teaching in the special operations program at the United States Naval Postgraduate School since 1993. He also serves as chairman of the Defense Analysis department. Dr. Arquilla’s teaching interests revolve around the history of irregular warfare, terrorism, and the implications of the information age for society and security. (“Cool War,” http://foreignpolicy.com/2012/06/15/cool-war/ 6/15/2012)

But now, somehow, it seems that war may no longer seem so terrible. How has this come to pass? The culprit is the bits and bytes that are the principal weapons of cyberwar. It is now possible to intervene swiftly and secretly anywhere in the world, riding the rails of the global information infrastructure to strike at one’s enemies. Such attacks can be mounted with little risk of discovery, as the veil of anonymity that cloaks the virtual domain is hard to pierce. And even when "outed," a lack of convincing forensic evidence to finger the perpetrator makes heated denials hard to disprove. Beyond secrecy, there is also great economy. The most sophisticated cyber weaponry can be crafted and deployed at a tiny fraction of the cost of other forms of intervention. No aircraft carriers needed, no "boots on the ground" to be shot at or blown up by IEDs. Instead, there is just a dimly lit war room where hacker-soldiers click for their country, and the hum of air conditioners keeping powerful computers from overheating. Cool room, cool war. The early returns seem to suggest the great efficacy of this new mode of conflict. For example, the Stuxnet worm, a complex program of ones and zeros, infected a sizeable proportion of Iran’s several thousand centrifuges, commanding them to run at higher and higher speeds until they broke. All this went on while Iranian technicians tried fruitlessly to stop the attack. The result: a serious disruption of Tehran’s nuclear enrichment capabilities — and possibly of a secret proliferation program. The sabotage occurred without any missile strikes or commando raids. And, for now, without any open acknowledgment of responsibility, although reporters and others have pointed their fingers at the United States and Israel. It is loose lips in high places, not sophisticated "back hacking," that seem to have divulged the secret of Stuxnet. Another example of the looming cool war is the malicious software known as Flame, which sought information via cyber snooping from target countries in the Middle East. The code that comprises it seems to make the point that we no longer need physical agents in place if we can now rely on artificially intelligent agents to dredge up the deepest secrets. There will be no new John le Carré to chronicle this era’s spies. Not when the closest thing to George Smiley is a few lines of source code. Beyond Stuxnet-like "cybotage" and software-driven spying, the coming cool war might also influence whether some traditional wars are even going to break out. The good news is that a preemptive cyber attack on the military command-and-control systems of two countries getting ready to fight a "real war" might give each side pause before going into the fight. In this instance, the hackers mounting such attacks should probably publicize their actions — perhaps even under U.N. auspices — lest the disputants think it was the enemy who had crippled their forces, deepening their mutual antagonism. There are no doubt some risks in having a third party mount a preemptive cyberattack of this sort — but the risks are acceptable when weighed against the chance of averting a bloody war. The other potential upside of cool war capabilities, in addition to tamping down military crises between nations, would lie in multilateral tracking of transnational criminal and terrorist networks. These villains thrive in the virtual wilderness of cyberspace, and it is about time that they were detected, tracked, and disrupted. Think of Interpol, or an international intelligence alliance, using something like Flame to get inside a drug cartel’s communications network. Or al Qaeda’s. The potential for illuminating these dark networks — and bringing them to justice — is great and should not be forgone. On balance, it seems that cyberwar capabilities have real potential to deal with some of the world’s more pernicious problems, from crime and terrorism to nuclear proliferation. In stark contrast to pitched battles that would regularly claim thousands of young soldiers’ lives during Robert E. Lee’s time, the very nature of conflict may come to be reshaped along more humane lines of operations. War, in this sense, might be "made better" — think disruption rather than destruction. More decisive, but at the same time less lethal. Against these potential benefits, one must also weigh the key downside of an era of cyber conflict: the outbreak of a Hobbesian "war of all against all." This possibility was first considered back in 1979 by the great science fiction writer Frederik Pohl, whose dystopian The Cool War — a descriptor that might end up fitting our world all too well — envisioned a time when virtually every nation fielded small teams of hit men and women. Their repertoires included launching computer viruses to crash stock markets and other nefarious, disruptive capabilities. In Pohl’s novel, the world system is battered by waves of social distrust, economic malaise and environmental degradation. Only the rebellion of a few cool warriors – some, but not all, were hacker types — at the end, offers a glimmer of hope for a way out and a way ahead. The question that confronts us today is whether to yield to the attractions of cyberwar. We have come out of one of mankind’s bloodiest centuries, and are already in an era in which wars are smaller — if still quite nasty. Now we have the chance to make even these conflicts less lethal. And in reality, there may be no option. Once the first network or nation takes this path — as some observers believe the United States is doing — others will surely follow, starting a new arms race, this time not in weaponry, but in clandestine and devastating programs like Stuxnet and the Flame virus. It is a curious irony that the United States, a power traditionally reluctant to go to war but furious in its waging, is now seemingly shifting gears. It is becoming a nation with the capability to go to war easily, while at the same time far less ferociously. Is this an improvement? Perhaps. Delaying Iranian proliferation with bits and bytes seems far superior to the costs and risks that would be incurred, and the human suffering inflicted, by trying to achieve such effects with bombs and bullets. But looking ahead, how will Americans respond when others begin to employ cyber means to achieve their ends, perhaps even by attacking us? After all, Stuxnet escaped from that Iranian facility into the wild, and is certainly being studied, reverse engineered and tweaked by many around the world. No country may be foolish enough to engage the incomparable U.S. military in open battle, but we seem like fairly easy pickings to the computer mice that may soon roar. Despite all these concerns, though, a cool war world will be a better place to live in than its Cold War predecessor. Yes, conflict will continue in the years to come, but it will morph in ways that make our self-destruction as a civilization less likely — even if it means living with occasional disruptions to vulnerable high-tech systems. The bargain made when "cyber" and "war" came together need not turn out to be Faustian. This story can still have a happy ending: As war becomes "cooler," ~~mankind’s~~ [humankind’s] future may edge a bit closer to the utopian end that all of us, secretly or not so secretly, truly desire.

### 2NC---No Escalation

#### **Their ev fearmongers**

Valeriano and Maness 15 – co-authors of Cyber War versus Cyber Realities, AND \*Senior Lecturer in Social and Political Sciences at the University of Glasgow, AND \*\*Visiting Fellow of Security and Resilience Studies at Northeastern University (Brandon and Ryan C., The Coming Cyberpeace: The Normative Argument Against Cyberwarfare, Foreign Affairs, https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace)

The era of cyberconflict is upon us; at least, experts seem to accept that cyberattacks are the new normal. In fact, however, evidence suggests that cyberconflict is not as prevalent as many believe. Likewise, the severity of individual cyber events is not increasing, even if the frequency of overall attacks has risen. And an emerging norm against the use of severe state-based cybertactics contradicts fear-mongering news reports about a coming cyberapocalypse. The few isolated incidents of successful state-based cyberattacks do not a trend make. Rather, what we are seeing is cyberespionage and probes, not cyberwarfare. Meanwhile, the international consensus has stabilized around a number of limited acceptable uses of cybertechnology—one that prohibits any dangerous use of force. Despite fears of a boom in cyberwarfare, there have been no major or dangerous hacks between countries. The closest any states have come to such events occurred when Russia attacked Georgian news outlets and websites in 2008; when Russian forces shut down banking, government, and news websites in Estonia in 2007; when Iran attacked the Saudi Arabian oil firm Saudi Aramco with the Shamoon virus in 2012; and when the United States attempted to sabotage Iran’s nuclear power systems from 2007 to 2011 through the Stuxnet worm. The attack on Sony from North Korea is just the latest overhyped cyberattack to date, as the corporate giant has recovered its lost revenues from the attack and its networks are arguably more resilient as a result. Even these are more probes into vulnerabilities than full attacks. Russia’s aggressions show that Moscow is willing to use cyberwarfare for disruption and propaganda, but not to inflict injuries or lasting infrastructural damage. The Shamoon incident allowed Iran to punish Saudi Arabia for its alliance with the United States as Tehran faced increased sanctions; the attack destroyed files on Saudi Aramco’s computer network but failed to do any lasting damage. The Stuxnet incident also failed to create any lasting damage, as Tehran put more centrifuges online to compensate for virus-based losses and strengthened holes in their system. Further, these supposedly successful cases of cyberattacks are balanced by many more examples of unsuccessful ones. If the future of cyberconflict looks like today, the international community must reassess the severity of the threat. Cyberattacks have demonstrated themselves to be more smoke than fire. This is not to suggest that incidents are on the decline, however. Distributed denial-of-service attacks and infiltrations increase by the minute—every major organization is probed constantly, but only for weaknesses or new infiltration methods for potential use in the future. Probes and pokes do not destabilize states or change trends within international politics. Even common cyber actions have little effect on levels of cooperation and conflict between states.

#### And, actors self-deter --- cyber is unique because defenders have the absolute defense of disconnecting. If attacks get strong enough, the internet itself becomes a bad deal for the defender, which also screws the attacker by denying lower-level cyber coercion and espionage

Jon **Lindsay and** Erik **Gartzke 14**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies, AND Erik Gartzke is Professor and Director of cPASS at the Department of Political Science @ UCSD, Lindsay, Jon R., and Erik Gartzke. “Coercion through Cyberspace: The Stability-Instability Paradox Revisited.” The Power to Hurt: Coercion in the Modern World, Oct. 2014.

Perhaps the simplest form of cross domain response to cyber threats is to forgo the use of the cyber domain altogether. While it is hard if not impossible to limit exposure to nuclear weapons and even a determined conventional assault, the risk of cyber attack can be completely eliminated by disconnection from digital networks. The internet is an artificial environment and connection to it is voluntary. Individuals, organizations, and states retain the ability to unplug completely, limit their online transactions, or erect various barriers to connection. Obviously disconnection is not very feasible commercially, socially, and militarily today, but this is more of an indicator of how positive the benefits of interconnection are compared to the perceived risks. If the risks were perceived as extreme, then firms and states could go back to making a living as they did before 1991 (when WWW went public). This is a cross-domain threat because it entails exiting the cyber domain altogether to leverage more traditional economic and military transactions. The threat of disconnection follows from the more general logic of international organizations, where contracts must be self-enforcing.44 On the internet as in institutions, ties among egoistic actors under anarchy must be mutually beneficial. If the internet is a bad deal for actors, they can throw up boundaries or exit cyberspace altogether. If repeated exposure to adversarial exploitation causes states to lose more than they gain from being online, then they can undermine the attacker’s very means for accessing the victim. The threat of voluntary disconnection is especially relevant for repeated interactions, or repeated exploitation, rather than a one-shot “bolt from the blue” cyber attack (which is better countered with cross-domain retaliation). The threat of disconnection is implicit in the voluntary nature of connection to the internet, and the potential loss of the ability to make future attacks exercises a deterrent effect on attacks in the present. An aggressor who does not want to lose the cyber adjuncts for espionage and disruption it has invested so much in developing will show restraint in their employment. This does not mean that coercion cannot take place online, but it is bounded by excess value. One implication is that the countries that can be most coerced on the internet will be those that have the most to lose by leaving it.

#### Attacks are too hard

Rebecca **Slayton 17**, Assistant Professor at Cornell University with a joint appointment in the Science and Technology Studies Department and the Judith Reppy Institute for Peace and Conflict Studies., Slayton, Rebecca. “What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.” International Security, vol. 41, no. 3, Jan. 2017, pp. 72–109.

Conclusion This article has shown that widespread claims about the offense dominance of cyberspace are fundamentally flawed; the offense-defense balance can be understood only in the context of specific adversaries with distinctive goals and levels of capability in managing complex information technology. In many cases, particularly those in which the goal is to achieve complex kinetic effects, cyber operations may well be less costly for the defense than the offense I have presented this argument in four parts. First, I have argued that conceptions of offensive advantage need to include valuations of the goals as well as the costs of cyber operations. The goals of cyber operations are much more varied than are battles for territory and may include propaganda, espionage, counter-espionage, and sabotage, in addition to assistance with territorial military operations. This article has focused on the relative utility of offense and defense—the value of the goals of offense less the costs of offense, and the value of the goals of defense less the costs of defense. A more complete analysis would consider expected utility—that is, it would include the probability of success for offense or defense as a function of offensive and defensive expenditures. The statistics for empirically predicting the probability of success for offense or defense under various conditions do not exist, however, and there is reason to doubt that such calculations will reach a useful level of accuracy or precision. Nonetheless, decisionmakers’ beliefs about the probability of success will shape behavior, and thus both theoretical and empirical analysis of the factors that make cyber offense and defense costly and valuable is crucial to informing policy. Second, I have theorized what makes cyber operations costly and valuable, arguing that the resulting offense-defense balance is a characteristic not of cyberspace, but rather of the relationship between two adversaries; the balance is not systemic, but dyadic. Although software does have an essential characteristic—arbitrary complexity—which provides the offense with many vulnerabilities to exploit, technology alone does not determine the balance. Nor is technology one of several independent factors to be summed up in a net assessment. Instead, it is the processes that govern the interactions between skilled users and technology that determine an organization’s readiness for offense or defense. Research on the capability maturity model shows that the cost of managing complex software decreases as the maturity of an organization’s processes increases. Nonetheless, cost grows with complexity. The skills and organizational capabilities needed for offense and defense are very similar, but offensive capabilities often require less coordination and therefore are less costly than defensive operations. Nonetheless, an offensive operation that aims to precisely control a complex system is much more difficult than one that merely aims to disrupt the system, and may be costlier than defense. Additionally, the advantages that complex software offers attackers diminish rapidly at the “edges” of cyberspace, where computers are used to control physical systems, because knowledge of the physical systems is needed to exercise careful control. Such knowledge is often tacit and therefore unavailable through cyber espionage. Thus, although information technology offers unprecedented efªciency for espionage, it is not the most cost-effective means of destruction. Cyberweapons are primarily advantageous for their covertness, and they become expensive when physical systems are the target.

#### There are diminishing returns on cyber escalation because stronger attacks are more likely to provoke disconnection.

Jon **Lindsay and** Erik **Gartzke 14**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies, AND Erik Gartzke is Professor and Director of cPASS at the Department of Political Science @ UCSD, Lindsay, Jon R., and Erik Gartzke. “Coercion through Cyberspace: The Stability-Instability Paradox Revisited.” The Power to Hurt: Coercion in the Modern World, Oct. 2014.

The combination of cross domain deterrence and voluntary connection to the internet gives rise to a variant of the classic stability-instability paradox. In Glenn Snyder’s original articulation of the paradox, mutually assured destruction could deter nuclear war. However, MAD was not credible for, and might even encourage, limited conventional war.56 Or as Robert Jervis puts it, “To the extent that the military balance is stable at the level of all-out nuclear war, it will become less stable at lower levels of violence.”57 Cyber capacity is a poor substitute for nuclear weapons, myths of paralysis notwithstanding, yet there is a similar logic constraining the distributions of harms which are possible via information technology. To extend this logic to the cyber domain, there are a variety of deterrent mechanisms contain the most disruptive types of cyber attacks yet fail to contain, and even enable, a wide variety of online espionage, subversion, symbolic protest, and criminal predation. In cyberspace we observe a rather stable damage contest (i.e., no “paralysis” and limited “disruption”) but a very unstable intelligence-counterintelligence contest (lots of “espionage” and “fraud” vying with efforts at “control” and “mobilization”). Thus the actors that have the ability to carry out highly destructive cyber attacks (mainly state actors for now) lack the motivation to attack; by contrast, these same actors as well as many different actors have both the ability and motivation to inflict irritant aggression with little fear of suffering consequences By and large, cyber options fill out the lower end of the conflict spectrum where deterrence is not as credible or reliable. The very few cases of physically disruptive cyber attack we do observe—mainly powerful states conducting covert action or battlefield support operations against militarily weaker opponents—have notably involved stronger actors who not only have the capacity to plan and conduct a sophisticated attack but also have the ability to deter retaliation against their use of cyber attack. This cyber variant of the stability-instability paradox has a slightly different logic, however. In the nuclear realm, actors cannot disconnect from the threatened harm, and this is what makes the threatened destruction both mutual and assured. When there are many missiles with many warheads, the chance of intercepting them on the ground through a disarming counterforce strike or in the air through ballistic missile defense with any confidence becomes vanishingly small. Not so in cyberspace, where connection to the internet or acceptance of connections through it is voluntary. There is “no forced entry in cyberspace” in Libicki’s phrase, and so the hundredth cyber attack against a closed vulnerability is as ineffective as the first. Attackers thus rely on deception to exploit vulnerabilities and ensure that they stay open. However, offensive deception can fail in the “fog of cyberwar” and defenders can be deceptive as well, both of which are more likely against high-reward targets (where cross domain deterrence also more credible). The need to preserve internet connections to facilitate ongoing and future deception as well as the need to preserve stealth to avoid the consequences of getting caught imposes discipline on attackers. Actors cannot enjoy the substantial benefits of interconnection without accepting some risk of exploitation (hacking to spy) and attack (hacking to disrupt). Thus the successful “lockout” of the internet, with advantage accruing exclusively to one political group or another, is not realistic. Moreover, because these harms share similar techniques, the observed abundance 39 of the former represents a latent potential for the later. The latent escalatory potential of even minor irritants leads to rampant fears of unrestrained catastrophe, to be sure. Yet this latent potential is difficult to harness for targeted coercion because the threat is self-effacing. Declared cyber threats that highlight the vulnerability to be exploited are readily mitigated. Instead, the ineradicable threat of cyber catastrophe (ineradicable as long as the internet continues to be useful) creates a general if diffuse deterrent effect among all parties who value their connection to the internet. No one who wants to make money on the internet really wants to have a cyberwar, and this includes states as well as criminals. Which types of actors are most able to benefit through internet coercion and which are most vulnerable to coercion? Large powers like the U.S. are highly dependent on the internet but also highly skilled at inflicting harm, both through cyber and traditional military force. Poor powers across the digital divide may have little vulnerability at all, while medium powers may have vulnerability but lack a range of forces to deter attacks. This might imply a “curvature” to the utility of cyber coercion. Big-capable countries are vulnerable to cyber harm but can deter through other military instruments. Poor states are not vulnerable. It may be the prosperous small or digitally developing who are in trouble, since they cannot credibly deter and have high dependence on the internet. The information revolution is often thought to be a boon to non-state actors, and indeed it is, but mainly in the irritant class of cyber operations. Moreover, the increasing ubiquity and sophistication of information technologies can be expected to have something of a democratizing effect on intelligence and counterintelligence techniques whereby firms and citizens will have access to and be concerned about the types of things that were historically the purview of obscure state intelligence agencies. However, it would be a mistake to use the increasing ferment of low-intensity information contests to infer the shape of higher 40 intensity activity. On the contrary, the traditional logic of war will continue to dominate the expression of cyber aggression. Because threatened internet harms depend on voluntary connections in the first place, and as many actors have alternative means to inflict (cross domain) harm in retaliation, the coercive utility of cyberspace is actually somewhat limited. At the same time an ever increasing variety irritants and more temperamental adjuncts becomes available for global political interaction. The “net” result is that opponents have strong incentives to impose costs via the internet but also to keep those costs low enough to preserve interconnection and avoid retaliation. Therefore, contests in damage will remain relatively stable while contests in intelligence will be increasingly unstable. The human-built world is becoming more complex, to be sure, but it is not necessarily more dangerous. As long as it is desirable to connect to the internet tomorrow, there will be only limited harm via the internet today.

### 2NC---AT: Miscalc

#### And, no miscalc­- cyber attacks will stay below the threshold of causing violence

Jon **Lindsay 15**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies., Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security, vol. 39, no. 3, Jan. 2015, pp. 7–47.

Exaggerated fears about the ~~paralysis~~ [deactivation] of digital infrastructure and growing concerns over competitive advantage exacerbate the spiral of mistrust. Closer consideration of domestic factors within China and China’s strategic interac- tion with the United States reveals a more complicated yet less worrisome situation. This article argues that for every type of purported Chinese cyber threat, there are also serious Chinese vulnerabilities and Western strengths that reinforce the political status quo. Cyberwar between the United States and China, much like U.S.-China conventional war, is highly unlikely. Nevertheless, the economically driven proliferation of information technology enables numerous instances of friction to emerge below the threshold of violence. From a technical perspective, cyber operations are often thought to be inexpensive and effective, but there are underappreciated institutional costs involved in their employment. Moreover, even if actors can overcome the operational barriers associated with ambitious cyber penetrations, they still have incentives to moderate the intensity of their exploitation in order to preserve the benefits that make exploitation worthwhile in the first place. This logic culminates in a relentlessly irritating but indefinitely tolerable stability in the cyber domain. China and the United States can look forward to chronic and ambiguous intelligence-counterintelligence contests across their networks, even as the internet facilitates productive exchange between them.

### 2NC---A2/AD Turn

#### We should make China as dependent on cyber as possible. They can’t punish us for it --- they haven’t practiced, hacking the US military is harder than it seems, and China’s bad at it

Jon **Lindsay 15**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies., Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security, vol. 39, no. 3, Jan. 2015, pp. 7–47.

Military Threats of Cyberwarfare Just as the social context of exploitation and adversary counteraction combine to blunt the potential of cyber espionage, similar challenges in operational weaponization and strategic interaction constrain the potency of more disruptive cyber threats. Yet conventional wisdom holds that a multitude of technical factors favor offense over defense in cyberspace and that the difªculty of attribution undermines the credibility of deterrence; therefore, weaker actors can attack the control systems of superior adversaries to achieve levels of physical disruption possible previously only through kinetic bombing. As President Obama writes in a Wall Street Journal opinion article, “Computer systems in critical sectors of our economy—including the nuclear and chemical industries—are being increasingly targeted. . . . In a future conºict, an adversary unable to match our military supremacy on the battleªeld might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger a ªnancial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we’ve seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill.”74 A number of former U.S. government ofªcials have even likened the advent of cyberweapons to a new atomic age and have wondered why a catastrophic cyberattack has not yet occurred.75 Chinese military doctrine similarly envisions cyberwarfare to be a low-cost, long-range, highly effective counter to a superior adversary.76 There are reasons, however, to doubt the PLA’s ability to implement these ideas or to defend itself against cyberattacks launched by a superior adversary. chinese cyber doctrine The aggressive tenor of Chinese writings on cyberwarfare and the copious APT activity described above are the major sources of evidence that Western analysts usually offer to characterize the Chinese cyberwarfare threat. Ofªcial Chinese military doctrine and sources in Chinese military professional literature consistently describe cyberwarfare as a revolutionary development in military affairs. Senior Col. Ye Zheng, author of books published by the Chinese Academy of Military Science entitled On Informationalized Warfare and Information Warfare Course, writes, “Although the main melody of the times—peace and development—is still playing strongly, the dark spirit of network warfare is lurking in the sky above humanity.” This rhetorical construction implies that the cyber revolution undermines Deng Xiaoping’s diagnosis of the largely stable nature of the international environment. Ye singles out the United States for experimenting with cyberweapons such as Stuxnet (used in the attack on Iranian enrichment infrastructure) and hints at the prospect of more to come: “[J]ust as nuclear war was the strategic warfare of the industrial age, network warfare will be the strategic warfare of the information age. It has already become a ‘top level’ form of operation that is highly destructive and relates to national security and survival.”77 He further describes cyberwarfare as an integral force multiplier as well as an instrument for achieving more strategic effects such as paralyzing another state’s economy or exerting psychological inºuence on entire populations. Similarly, an author in the PLA’s Science of Information Operations writes that cyber strikes “can seek to achieve partial or large-scale paralysis of enemy systems. As soon as a virus enters the enemy’s command and control system, it will have tremendous destructive impact. . . . Therefore computer network war is an important means for paralyzing the enemy in wars of the future.”78 The PLA recognizes the existence of an “information domain” (xinxi lingyu), although as with “information security” it encompasses a wider range of subcategories to include computer network and electronic warfare as well as psychological and intelligence operations.79 Information operations are con-sidered so vital for the limited high-technology wars the PLA envisions ªghting that information supremacy is thought to be a precondition for gaining military supremacy anywhere else. The PLA’s general strategic principle of “active defense” stresses offensive operations to seize the initiative. The authoritative Science of Campaigns thus states that the beginning of a network war will determine its outcome: “Whoever strikes ªrst prevails.”80 PLA strategists assert that the vital targets of an advanced technology adversary are its information systems, and by attacking them covertly from beyond the range of enemy weapon systems it is possible to cause paralysis of the enemy’s organization, strategic decisionmaking, and national economy. As an important article by Gen. Dai Qingmin on the concept of “integrated network-electronic warfare” points out, “Information operations in high-tech warfare are, to a very great extent, a struggle which revolves around the destruction and the protection of C4ISR systems.”81 Chinese writers argue that a relatively weaker PLA can achieve information superiority against a stronger military only as long as it is able to launch paralyzing strikes at the beginning of a conºict. The Chinese perspective on using information technology to improve awareness, synchronization, and precision is inspired by 1990s-era American writings about the “revolution in military affairs [RMA].”82 RMA ideas were themselves inspired by Soviet strategists, and the common Marxist-Leninist belief that “technology determines tactics” surely inºuences PLA thought.83 Yet the most recent and relevant inspiration comes from Chinese study of U.S. operations in Iraq and the Balkans and analysis of the U.S. military’s heavy dependence on communication and logistics networks.84 In particular, the accidental U.S. bombing of the Chinese embassy in Belgrade prompted President Jiang Zemin to direct the PLA to develop so-called assassin’s mace (shashoujian) weapons to solve the problems of “seeing far, striking far, and striking accurately.” Jiang reasoned that “what the enemy is most fearful of is what we should be developing.”85 As the consummately “network centric” U.S. military leverages data links to reduce its force size—substituting information for mass in the RMAformula for success—those links become vulnerabilities and thus tempting targets for the PLA. Insofar as the cyber revolution thesis is inºuential in U.S. strategic planning, moreover, the specter of PLA cyberwarfare may indeed have some success in creating fear and encouraging restraint in U.S. planning. Remarkably, however, there appears to be little mention in Chinese writings of the considerable controversy over the RMA in Western strategic literature or considerations of the downsides of the RMA.86 The United States has fought several regional wars in recent decades and in the process has experienced no small amount of confusion and the “fog of war” as computer systems break down unexpectedly, adversaries refuse to conform to the assumptions of network-centric doctrine, and service members resort to ad hoc improvisations to muddle through. The PLA, by contrast, has not had the opportunity to test its ideas of “integrated network electronic warfare” in combat, and realistic command and control training is notoriously hard to achieve absent interaction with a real enemy and complex environment. The following review of Chinese cyber capabilities suggests that similar skepticism is also warranted for Chinese cyberwarfare. chinese cyber capabilities Although Chinese writers emphasize the revolutionary potential of cyberwarfare, episodes of Chinese aggression in cyberspace have been more mundane. China’s “hacker wars” ºare up during episodes of tension in Chinese foreign relations, as between Taiwan and the mainland between 1996 and 2004 in the wake of Taiwanese elections, between the United States and China following the 1999 bombing of the Chinese embassy in Belgrade and the 2001 EP-3 spy plane collision, and between China and Japan throughout the past decade during controversies involving the Yasukuni Shrine and the Senkaku/ Diaoyu Islands.87 Nationalist hackers (as distinguished from PLA units) deface foreign websites and launch temporary distributed denial of service attacks. Nationalist online outbursts may take place with the tacit consent or encouragement of the Chinese government, yet patriotic “hacktivism” is essentially just another form of symbolic protest. There has been speculation that PLA “cyber militias” associated with Chinese universities maintain a more potent reserve capability, but one study of open sources suggests that they are oriented toward more mundane educational and network defense activities.88 The majority of known PLA cyber operations are CNE for intelligence rather than computer network attacks to cause disruption.89 Nevertheless, many analysts worry that CNE is “only a keystroke away” from CNA, thereby generating dangerous ambiguity between intelligence gathering and offensive operations. Intrusion techniques developed for industrial espionage might be used to plant more dangerous payload code into sensitive controllers or constitute reconnaissance for future assaults. Chinese probing of critical infrastructure such as the U.S. power grid is aggressive, to be sure, so a latent potential for the PLA to convert CNE into CNA cannot be discounted.90 The discovery of access vectors and exploitable vulnerabilities, however, is only the first step to achieving effective reconnaissance of a target, and effective reconnaissance is just one step toward planning and controlling a physically disruptive attack. The most signiªcant historical case of kinetic CNA to date, the Stuxnet attack on Iran’s enrichment infrastructure, suggests that painstaking planning, careful rehearsals, and sophisticated intelligence are required to control a co- vert disruption.91 The U.S. military also considered using cyberattacks to take down Libya’s air defense system in 2011, but reportedly it would have taken too long to develop the option.92 The latency between CNE and CNA is more complicated than generally assumed.

#### Seriously, they’re totally uncoordinated and terrible

Jon **Lindsay 15**, Jon R. Lindsay is an assistant research scientist at the University of California Institute on Global Conflict and Cooperation and an assistant adjunct professor at the University of California, San Diego School of International Relations and Pacific Studies., Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security, vol. 39, no. 3, Jan. 2015, pp. 7–47.

china’s fragmented cyber defenses The CCP’s obsession with political “information security” has so far not translated into effective technical “network security.”34 Cybercrime thrives amid a fragmented bureaucracy. Lax and uneven law enforcement emboldens Chinese cybercriminals to prey on domestic targets and creates a blatantly open online underground economy in China. Chinese cybercriminals target Chinese victims given the relatively low risk of domestic police action; by comparison, Eastern Europe cybercriminals tend to avoid hacking at home, instead focusing their predation abroad. Stolen usernames and passwords, ªnancial data, video game accounts, and hacker tools can be bought and sold openly on Chinese social media forums such as Baidu and Tencent QQ. By one estimate, cybercrime damage to the economy exceeded $830 million and affected more than 20 percent of users and websites in 2011 alone.35 Rampant cybercrime is a result, in part, of China’s below-average cyber defenses.36 Importantly, networks exposed to criminal predation are also vulnerable to foreign exploitation, because state intelligence services use some of the same technology and methods. Cyber policy coordination among defense, law enforcement, and regulatory agencies is a challenge in any state, but China’s lack of governmental transparency makes a hard problem worse. Prior to 2014, primary responsibility for cybersecurity policy resided in a subcommittee of the CCP State Informatization Leading Group (SILG), formed in 2001 to guide national information technology development or “informatization” (xinxihua) and chaired by the CCP premier. SILG’s early focus on cybersecurity was eclipsed by the Chinese elite’s preoccupation with the 2008 Beijing Olympics and ªnancial crisis, leaving regulatory agencies and newly funded companies to their own devices. SILG updated its guidance criteria in 2012 to reºect renewed concerns about critical infrastructure and privacy, but elite focus remained sporadic. In February 2014, amid tension stemming from the Snowden leaks, the CCP announced the creation of the Cybersecurity and Informatization Leading Group (CILG), chaired by Xi Jinping (with twenty-one other Politburo or ministeriallevel ofªcials on the roster).37 The CILG aids Xi’s efforts to tighten Party discipline and respond to foreign cyber threats.38 Greater attention by China’s elite via CILG may improve cyber policy coordination, but prior experience does not bode well. In China, as in other states, a large and diverse set of public and private entities has a stake in the making of cyber policy, yet the steady stream of cyber friction does not add up to sustained elite pressure for reform. Policy elites with more pressing priorities usually do not focus consistent pressure on a heterogeneous set of bureaucratic interests.39 Numerous agencies under the State Council are responsible for the implementation of policy and the regulation of information technology in China. The People’s Liberation Army, subordinate to the CCP rather than the state, has considerable military and intelligence cyber capacity as well as civilian regulatory responsibility (e.g., in the transportation sector). Provincial governments, furthermore, enjoy substantial de facto autonomy and compete ªercely for patronage. In response to a glut of funding for SILG initiatives, expenditure in China’s information security industry grew from $527 million in 2003 to $2.8 billion in 2011. In the assessment of one industry observer, however, this expansion was marred by a “lack of overall planning,” “decentralization of decisionmaking power,” and a “lack of adequate communication.”40 As in other areas of Chinese policy, the implementation of cybersecurity is disjointed functionally and regionally, rife with rent seeking by bureaucratic agencies and enterprises. Haphazard interagency cooperation and industrial regulation create a permissive environment for cybercrime, which saps the potential of e-commerce and user trust in online services.

## Solvency

### 1NC---Defense

#### Developing trust in AI is impossible---black box problem means true integration is impossible

Erik Lin-Greenberg 20, postdoctoral fellow at the University of Pennsylvania’s Perry World House. Texas National Security Review, Vol 3, Iss 2. Spring. "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making" <https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/> //pipk

AI can also strain alliance decision-making by fueling uncertainty about information and military actions. Unlike human analysts or military personnel who can be asked to explain and justify their findings or decisions, AI generally operates in a “black box.” 97 The neural networks that underpin many cutting-edge AI systems are opaque and offer little insight into how they arrive at their conclusions.98 These networks rely on deep learning, a process that passes information from large data sets through a hierarchy of digital nodes that analyze data inputs and make predictions using mathematical rules. As data flows through the neural network, the net makes internal adjustments to refine the quality of outputs. Researchers are often unable to explain how neural nets make these internal adjustments. Because of this lack of “explainability,” users of AI systems may have difficulty understanding failures and correcting errors.99

Policymakers have called for the development of more transparent AI systems, and researchers are working to develop explainable AI tools that peer inside the AI black box.100 Yet, many decision-makers remain uncomfortable with the uncertainty surrounding AI-enabled systems. The commander of the U.S. Air Force’s Air Combat Command, for instance, publicly explained that he was not yet willing to rely on AI programs to analyze the full-motion video collected by reconnaissance drones. He argued that although systems are improving, they are still unable to consistently provide accurate analysis.101 So long as the decisions and analysis of AI systems remain opaque, military commanders may be reluctant to trust AI-enabled systems. And if used, AI may contribute to the fog of war, rather than reduce it, making it difficult to make decisions using information delivered by AI technologies.

The operational implications associated with uncertainty and lack of trust in AI would likely be exacerbated in multinational alliance contexts. There is significant cross-national variation in trust in AI technologies, even among close allies. One 2018 survey, for instance, found that just 13 percent of respondents in Japan and 17 percent of respondents in South Korea trust artificial intelligence, compared to 25 percent of respondents in the United States. Similar disparities exist between the United States and many of its NATO allies. In Spain, 34 percent of respondents trust artificial intelligence, compared to 21 percent in Canada, 40 percent in Poland, and 43 percent in Turkey.102 Given this variation, policymakers and commanders from some states may be more reluctant to use AI-enabled systems or trust the information they deliver than leaders from other states during multinational operations.

Allied decision-makers will also face uncertainty when confronting a rival’s use of AI-enabled technologies. Leaders will be forced to wrestle with whether to respond to actions carried out by AI-enabled systems — like autonomous aircraft or ships — in the same way as actions carried out by traditionally manned assets. Existing doctrine and law are generally silent on these issues, providing no guidance on the appropriate response. States have drafted domestic policies to govern their own use of autonomous weapon systems, but these regulations and international law make no distinction between how states should react to a rival’s AI-enabled military actions versus “traditional” military actions.103 Yet, decision-makers may believe that a rival’s use of AI technologies demands different responses than those involving manned platforms.104 What happens if a rival claims that an attack carried out by an AI-enabled system was the result of a flawed algorithm? Should air defense forces respond differently to an adversary’s autonomous drones that penetrate friendly airspace than to a manned aircraft that does the same? Decision-makers may find themselves with little time to consider these complicated issues, particularly as AI technology accelerates the speed of a rival’s military operations.

#### Data sharing is too hard---integration is impossible

Erik Lin-Greenberg 20, postdoctoral fellow at the University of Pennsylvania’s Perry World House. Texas National Security Review, Vol 3, Iss 2. Spring. "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making" <https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/> //pipk

Data Sharing and Standardization

As the number of states that employ military AI applications grows, the ability of allies to operate collectively will depend, in part, on the sharing of data that fuels AI systems. AI requires massive amounts of data to train and feed algorithms and models. To identify a surface-to-air missile site, for instance, an AI image classifier must learn to differentiate missile sites from other facilities by studying images of known missile sites. The more data used to train these systems, the more accurate the system will be.66 Once fielded, AI-enabled systems like the image classifier must continue to be fed imagery from reconnaissance aircraft, satellites, or other assets in a format that allows for target identification. Shared data might be needed to enhance the accuracy of AI-enabled systems or to increase the effectiveness of multinational operations. For example, some member states may be better positioned than others to gather data on a shared rival, increasing the amount of data available to AI systems.67

Because of its central role in AI development and operations, the U.S. military has described data as a “strategic asset,” yet sharing data — even within the U.S. military — has posed a significant challenge.68 Lt. Gen. Jack Shanahan, founding director of the Department of Defense’s Joint Artificial Intelligence Center, lamented that data “has stymied most of the [military] services when they dive into AI.” Specifically, “they realize how hard it is to get the right data to the right place, get it cleaned up, and train algorithms on it.”69 There are two primary factors that underlie these challenges. First, data resides in thousands of different repositories and often lacks standardized formatting. Video from the U.S. military’s fleet of reconnaissance aircraft, for instance, is stored on multiple separate networks and in different data formats. Second, significant amounts of data collected by weapons and sensor systems are considered proprietary by the contractors that design and maintain the equipment. Firms must first release or “unlock” this data before it can be analyzed or fed into other systems.70

Although shared data is needed to develop AI technologies that can integrate with allied equipment, states face both political and technical barriers to sharing security sector information. From a political standpoint, even the closest allies may be hesitant to share the sensitive data that undergirds military AI systems. States fear that sharing sensitive data might reveal intelligence sources and methods, the revelation of which could compromise ongoing operations or strain political relationships. During the Vietnam War, for example, the United States was hesitant to share intelligence with its ally South Vietnam. Officials feared that communist sympathizers in the ranks of South Vietnam’s military and intelligence services would pass information to North Vietnam and the Vietcong. They were also concerned that intelligence might highlight that the United States was planning operations that did not align with South Vietnam’s government priorities.71 States also worry that shared information could be used for purposes other than initially intended or in ways that are at odds with the sharing state’s interests. Turkey, for instance, may have used intelligence shared as part of counter-Islamic State operations to instead target Kurdish forces in northern Syria.72

To minimize these perceived risks, states often impose restrictions on information sharing. One of the most common control measures is sharing only finished intelligence — products such as briefings or reports derived from a variety of different intelligence sources.73 These products provide assessments, but generally omit technical data — like details about the information source — that could reveal intelligence-gathering procedures and methods. Although data sharing is a type of intelligence sharing, developing and operating AI-enabled systems may require the exchange of more complete raw data in far larger quantities than traditional intelligence sharing. Raw data, which includes imagery files and signals intercepts, can include metadata such as spectral signatures of imagery or characteristics of electronic emissions that can be used to feed AI systems.74 Since this information can expose precise capabilities and shortcomings of a state’s intelligence systems, decision-makers may be hesitant to share it — especially in the large quantities needed to develop and run many AI-enabled systems.

There are also technical obstacles to data sharing. Just as the U.S. intelligence community and military stores information in nonstandardized formats on multiple systems, so too do national security institutions in other allied states. Across an alliance, the same type of data might reside on hundreds of different networks and in different formats, making it difficult to share data or to develop interoperable systems. To use data from other alliance partners, data must first be located, transferred out of a state’s classified computer network, and reformatted into a standardized, usable form. Given that the U.S. military has faced significant data management challenges in its own AI development, we should expect alliances — with their greater number of institutional actors and data sources — to encounter even greater obstacles to data sharing.

Vulnerabilities: AI and Data

In addition to barriers to sharing, allies face the possibility that the data that they do share may be especially vulnerable to adversary manipulation. Engineers and military leaders worry that rivals could hack into data repositories and “poison” data — inserting fake data or making existing data deliberately flawed.75 In one recent academic study, researchers used data poisoning to cause an algorithm designed to identify street signs to misclassify stop signs as speed limit signs.76 In the military domain, a rival could poison imagery data in order to throw off AI target recognition systems, leading the system to miss military targets, classify them as nonmilitary ones, or identify civilian infrastructure as military facilities. At best, this could require manpower-intensive efforts to secure and sanitize data or lead states to turn back to manual analysis of targets. At worst, this could lead to the inadvertent targeting of noncombatants.

While the risk of data poisoning plagues all AI users, alliance military operations may be particularly susceptible because data inputs from multiple states are used to train and operate AI-enabled systems across the alliance. Flawed data inputs from one state can therefore have cascading effects across an alliance’s operations. Rivals will recognize that different members of an alliance defend their networks and data with different levels of safeguards. As a result, rivals may target data stored by states where they have easier access.77

#### There’s not enough AI workers to solve---shortages means innovations won’t be effective

Stefano Costalli 21, Associate Professor of Political Science in the Department of Political and Social Sciences, University of Florence, Italy and Research Fellow of the Michael Nicholson Centre for Conflict and Cooperation, University of Essex. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

A key requisite for all organizational innovations to occur and for Big Data analysis to be effective is the development and incorporation of a Big Data culture. Chief data officers and senior data-related leadership positions will acquire crucial importance in the analysis of information and in the actual decision-making process, but these positions require a special mix of talent and tools that are currently scarce in many large organizations, especially in the public sector. The organizations that are implementing big data analysis seem especially in need of ‘translators’ – professionals that can ensure effective communication between the Big Data analysis unit and other parts of the organization, where workers are not data scientist and may not be ready to work directly on complex models. However, organizations willing to use Big Data are also in need of real data scientists and analysts, because sophisticated techniques and data analysis tools eventually rely on talented humans who know how to manage the tools and interpret data. As a result, attracting new types of talented young workers and retaining them creating new career paths and opportunities will represent both an essential organizational innovation and an important challenge.

In fact, some members of the WG highlighted that it will not even be easy to find many workers with the appropriate knowledge and skills to perform the new tasks in old and complex organizations. It is possible to find computer scientists, but sometimes these individuals do not seem to fit well with large organizations whose main core business has not much to do with computer science. At the moment, it is even more difficult to find translators, since in principle these workers should be social scientists with an expertise in Big Data analysis, but most academic institutions are not ready to forge these profiles. For what concerns NATO and national armed forces, this educational task is not even performed by military academies, even though some experiments are emerging. The ideal profile would include technical awareness, quantitative analytical skills, broad vision, flexibility and open-mindedness – and this explains why it is not easy to produce it.

### 1NC---R&D Tradeoff Turn

#### AI trades off with other federal R&D

Christie Lawrence & Sean Cordey 20, concurrent Master of Public Policy and Juris Doctorate 2024 candidate at Harvard Kennedy School and Stanford Law School and recipient of Harvard Kennedy School’s John F. Kennedy Fellowship. She previously worked as a management consultant for Oliver Wyman where she focused on regulatory risk and global data protection for financial institutions. She also worked at the Department of State. Her research with the Belfer Cyber Project includes AI policy, cybersecurity, US-Russian cyber relations, and US foreign policy in the digital age. a dual Master degree in International Affairs candidate at the Fletcher School of Law and Diplomacy and the University of St. Gallen and was a Belfer Cyber Security Project research assistant. He previously worked for the Swiss ministry of foreign affairs in Washington D.C. and currently works as a researcher for the Cyber Defense Project at the Center for Security Studies (CSS) at the ETH Zürich. The Cyber Project Belfer Center for Science and International Affairs Harvard Kennedy School. "The Case for Increased Transatlantic Cooperation on Artificial Intelligence" August. <https://www.belfercenter.org/sites/default/files/2020-08/TransatlanticAI.pdf> //pipk

AI Funding: Although the Administration has pledged to increase (non-defense and defense) AI-related spending and absolute AI R&D budget numbers have increased, there are concerns that these numbers may not accurately reflect development. First, as AI-related expenditures have increased, the budget for all government R&D has decreased.158 For example, the President’s budget request for cuts in R&D at NSF, NIH, DOE, and other agencies, would force these government entities to prioritize AI R&D to the detriment of other, potentially equally useful R&D.159 Second, without full transparency about the procedures undertaken to re-classify projects as AI-related, it is not possible to fully credit the supposed increase in AI-related R&D to new AI projects. One analysis by Bloomberg Government of the Pentagon’s FY2020 budget found that approximately 27% of the legacy AI-related activities had not included any AI components or descriptors in the previous year budget.160, 161 Observers have suggested that the DoD was partaking in “AI-washing,” or exaggerating the increase in its AI-related R&D to meet government imposed objectives. 162 The US government will need to be careful that initiatives to enhance AI innovation do not foster a zero-sum competition between AI and other S&T research but instead foster genuine innovation.

#### Federal research solves cancer

Doudna & Marson 17 (Jennifer & Alex. Jennifer Doudna is a professor of chemistry, and molecular and cell biology, at the University of California, Berkeley. Alex Marson is an assistant professor of microbiology, immunology, and medicine at UC San Francisco. "Federal funding for basic research led to the gene-editing revolution. Don't cut it" <https://www.vox.com/the-big-idea/2017/4/22/15392912/genes-science-march-nih-funding-basic-research-doudna>) \*edited for language

Labs across our country are a source of American optimism — advancing knowledge, technologies, and cures. And yet, as citizens in 500 cities worldwide prepare to march this weekend in support of science, many American scientific practitioners are afraid. They worry that American science as we know it would be ~~hobbled~~ [hurt] if President Trump’s proposed 18 percent cut to the National Institutes of Health, America’s premier medical research funder, becomes reality. We hope Congress will hear history’s call and re-assert American leadership in advancing humanity’s scientific knowledge. Call us naïve, but we believe — as an immunologist and biochemist attempting to perfect and deploy gene-editing advances to cure disease — that Democrats and Republicans alike can be united by a shared drive for scientific exploration and life-saving discoveries. Science is not the property of any political party or region of the country. In red states and blues states, daughters and sons ask their first scientific questions when they come to us and wonder how the human body grows, how genes are inherited, and how a medicine works. Over the past century, American political leaders have encouraged young people to ask these fundamental questions, invested in their training to become scientists, and given them tools to translate questions into innovation. The rewards of breakthroughs are felt most acutely when our families experience illness. Many of us know the pain of a loved one discovering a lump that turns out to be cancer or showing signs of neurological decline. In these moments, whatever our politics, we all hope to reach for the most powerful medicines, which continue to result from the relentless pursuit of scientific knowledge. Gene editing will lead to major breakthroughs in combating disease As we write, biomedical progress is accelerating, changing how we understand and fight disease. One example is CRISPR, a tool that can edit specific sequences in human DNA, which one of us helped invent and the other uses in research to understand and control the human immune system. Targeted at the building blocks of life, CRISPR could induce immune cells to fight disease or neutralize predisposition to one. The combination of CRISPR and new therapies has raised hopes for a new generation of powerful cancer treatments. Across the US, our colleagues are teaming up and racing to apply similar approaches to dementia, heart disease, and countless other conditions. A growing number of Americans have heard of CRISPR and its medical potential. Far fewer realize that the transformative applications of CRISPR genome editing would never have occurred without robust funding for basic scientific research. Inquiry into unusual genes in unglamorous bacteria before we even knew the gene-altering power they contained, laid the foundation for CRISPR technology. Now that same technology is driving a revolution in biomedicine and rapidly advancing towards clinical trials. We certainly have not charted the breadth of microorganisms that will inspire the invention of future drugs, nor fathomed the full complexity of the inner workings of human cells. That’s the work of basic scientific research. The next revolution in biology is currently an idea in a scientist’s head, or being hashed out in a late night lab conversation among graduate students, or sitting in a grant application to the NIH asking for a chance. Our research represents just a sliver of the vital projects that more than 300,000 researchers are undertaking in 50 states with NIH support. Unfortunately, the president’s proposed budget threatens that research. Among the deep cuts to science support he seeks is a nearly $6 billion reduction for NIH, representing nearly a fifth of the agency’s funding. (For context, that’s more than its entire current cancer budget.) The proposal has prompted justifiable concern among scientists and patient advocates. Funding cuts would deter tomorrow’s scientists from the field, or at least from pursuing careers in the US. Curtailing the NIH budget, a significant chunk of America’s biomedical research funding, would cripple our capacity to lead on pressing health challenges. The vast majority of NIH funds go to funding scientific research and training, both within the agency and externally. For decades, America has been at the forefront of scientific innovation. Slashing funding would destroy long-term projects and threaten American primacy in medical research. More importantly, underfunding NIH will hamstring efforts to fight disease. By funding basic research, the federal government lays the groundwork for future innovation Some might argue that private industry will fill the void, given the economic benefits of scientific breakthroughs,. But the truth, surprising to many, is that while private investment can indeed lead to the discovery of profitable new drugs and therapies, its focus on the bottom line tends to short-change basic — as opposed to applied —research. In weighing a project’s anticipated earnings and costs, businesses seek a probable path to profit. Transformative science requires a different mold than the one found in industry. CRISPR grew not out of a race to develop disease treatments, but out of basic scientific research into bacteria. The boldest innovations stem from unlikely collaborations or quixotic investigations — in other words, exploration driven by discovery rather than profit. Occasionally, these projects do become profitable, but only through a scientist’s persistent drive to show that an idea, a hope, a hunch, is not so crazy after all. While stockholders may not want a corporation to make bets that are unlikely to have an immediate payoff, as citizens we must demand our government does so. And that’s precisely why the National Institutes of Health exists: It ensures that, though we may not know what the next CRISPR will be, there are bright and dedicated American scientists pursuing many roads of inquiry, even if the path to profit isn’t immediately clear. As Congress considers the president’s budget, we have a simple request: Please give America’s scientists the tools we need to succeed. Supporting NIH will position American scientists to continue the open-ended explorations at which they excel. Government funding is critical to encourage our scientists to pursue not just the challenges that are relatively easy, or obviously profitable, but the ones that are fiendishly hard —yet crucial. NIH funding is a down payment on discovery, the seed money to fund a critical step toward ending Alzheimer’s or curing cancer. What could be a bigger “win” for America than that?

#### Extinction

Johnson 16 – George Johnson, columnist and science journalist for the New York Times, M.A. in Journalism and Public Affairs, American University (“Scientists Ponder the Prospect of Contagious Cancer,” *New York Times*, February 22nd, https://www.nytimes.com/2016/02/23/science/scientists-ponder-the-prospect-of-contagious-cancer.html?mcubz=0)

For all its peculiar horror, cancer comes with a saving grace. If nothing else can stop a tumor’s mad evolution, the cancer ultimately dies with its host. Everything the malignant cells have learned about outwitting the patient’s defenses — and those of the oncologists — is erased. The next case of cancer, in another victim, must start anew. Imagine if instead, cancer cells had the ability to press on to another body. A cancer like that would have the power to metastasize not just from organ to organ, but from person to person, evolving deadly new skills along the way. While there is no sign of an imminent threat, several recent papers suggest that the eventual emergence of a contagious human cancer is in the realm of medical possibility. This would not be a disease, like cervical cancer, that is set off by the spread of viruses, but rather one in which cancer cells actually travel from one person to another and thrive in their new location. So far this is known to have happened only under the most unusual circumstances. A 19-year-old laboratory worker who pricked herself with a syringe of colon cancer cells developed a tumor in her hand. A surgeon acquired a cancer from his patient after accidentally cutting himself during an operation. There are also cases of malignant cells being transferred from one person to another through an organ transplant or from a woman to her fetus. On each of these occasions, the malignancy went no further. The only known cancers that continue to move from body to body, evading the immune system, have been found in other animals. In laboratory experiments, for instance, cancer cells have been transferred by mosquitoes from one hamster to another. And so far, three kinds of contagious cancers have been discovered in the wild — in dogs, Tasmanian devils and, most recently, in soft shell clams. The oldest known example is a cancer that spreads between dogs during sexual intercourse — not as a side effect of a viral or bacterial infection, but rather through direct conveyance of cancer cells. The state of the research is described in a review, “The Cancer Which Survived,” published last year by Andrea Strakova and Elizabeth P. Murchison of the University of Cambridge. The condition, canine transmissible venereal tumor disease, is believed to have sprung into existence 11,000 years ago — as a single cell in a single dog — and has been circulating ever since. (Why did this happen in dogs and not, say, cats? Perhaps because of what the authors demurely call the dogs’ “long-lasting coital tie” — the half an hour or so that a male and female are locked in intercourse, tearing genital tissues and providing the cancer cells with a leisurely crossing.) Normally a cancer evolves in a single body over the course of years or decades, accumulating the mutations that drive it to power. But to have survived for millenniums, researchers have proposed, canine cancer cells may have developed mechanisms — like those in healthy cells — to repair and stabilize their own malignant genomes. Early on, cancer cells typically flourish by disabling DNA repair and ramping up the mutational frenzy. Somewhere along the way, the age-old canine cells may have reinvented the device to extend their own longevity. There is also speculation that this cancer may have learned to somehow modify canine sexual behavior in ways that promote the disease’s spread and survival. The second kind of contagious cancer was discovered in the mid-1990s in Tasmanian devils, which spread malignant cells as they try to tear off one another’s faces. Though it may be hard to sympathize, devil facial tumor disease threatens the creatures with extinction. With so few examples, transmissible cancer has been easy to dismiss as an aberration. But in December, scientists at the Universities of Tasmania and Cambridge reported in Proceedings of the National Academy of Sciences that Tasmanian devils are passing around another kind of cancer — genetically distinct from the first. It’s weird enough that one such cancer would arise in the species. What are the chances that there would be two? One theory is that the animals are unusually vulnerable. Driven so close to extinction — by climate change, perhaps, or human predators — the species is lacking in genetic diversity. The cells of another devil injected through a vicious wound may seem so familiar that they are ignored by the recipient’s immune system. If some of the cells carry the mutations for the facial cancer, they might be free to flourish and develop into a new tumor. But the scientists also proposed a more disturbing explanation: that the emergence of contagious cancer may not be so rare after all. “The possibility,” they wrote, “warrants further investigation of the risk that such diseases could arise in humans.” Cancer has probably existed ever since our first multicellular ancestors appeared on Earth hundreds of millions of years ago. The life spans of even the longest-lived animals may be just too brief for cancers to easily evolve the ability to leap to another body. Otherwise, contagious cancer would be everywhere.

### 2NC---Innovation Impact

#### Extinction—innovation is the only way to avoid tipping points.

Naam, fellow of the Institute for Ethics and Emerging Technologies, 13

(Ramez, former Microsoft executive, "How Innovation Could Save the Planet", World Future Society, The Futurist, 2013 Issues of The Futurist, March-April 2013 (Vol. 47, No. 2), www.wfs.org/futurist/2013-issues-futurist/march-april-2013-vol-47-no-2/how-innovation-could-save-planet)

The Best of Times: Unprecedented Prosperity There are many ways in which we are living in the most wonderful age ever. We can imagine we are heading toward a sort of science-fiction utopia, where we are incredibly rich and incredibly prosperous, and the planet is healthy. But there are other reasons to fear that we’re headed toward a dystopia of sorts. Ramez Naam spoke at WorldFuture 2013, the annual conference of the World Future Society in Chicago, in July of 2013. On the positive side, life expectancy has been rising for the last 150 years, and faster since the early part of the twentieth century in the developing world than it has in the rich world. Along with that has come a massive reduction in poverty. The most fundamental empowerer of humans—education—has also soared, not just in the rich world, but throughout the world. Another great empowerer of humanity is connectivity: Access to information and access to communication both have soared. The number of mobile phones on the planet was effectively zero in the early 1990s, and now it’s in excess of 4 billion. More than three-quarters of humanity, in the span of one generation, have gotten access to connectivity that, as my friend Peter Diamandis likes to say, is greater than any president before 1995 had. A reasonably well-off person in India or in Nigeria has better access to information than Ronald Reagan did during most of his career. With increased connectivity has come an increase in democracy. As people have gotten richer, more educated, more able to access information, and more able to communicate, they have demanded more control over the places where they live. The fraction of nations that are functional democracies is at an all-time high in this world—more than double what it was in the 1970s—with the collapse of the Soviet Union.\* Economically, the world is a more equal place than it has been in decades. In the West, and especially in the United States, we hear a lot about growing inequality, but on a global scale, the opposite is true. As billions are rising out of poverty around the world, the global middle classes are catching up with the global rich. In many ways, this is the age of the greatest human prosperity, freedom, and potential that has ever been on the face of this planet. But in other ways, we are facing some of the largest risks ever. The Worst of Times: The Greatest Risks At its peak, the ancient Mayan city of Tikal was a metropolis, a city of 200,000 people inside of a civilization of about 20 million people. Now, if you walk around any Mayan city, you see mounds of dirt. That’s because these structures were all abandoned by about the mid-900s AD. We know now what happened: The Mayan civilization grew too large. It overpopulated. To feed themselves, they had to convert forest into farmland. They chopped down all of the forest. That, in turn, led to soil erosion. It also worsened drought, because trees, among other things, trap moisture and create a precipitation cycle. When that happened, and was met by some normal (not human-caused) climate change, the Mayans found they didn’t have enough food. They exhausted their primary energy supply, which is food. That in turn led to more violence in their society and ultimately to a complete collapse. The greatest energy source for human civilization today is fossil fuels. Among those, none is more important than oil. In 1956, M. King Hubbert looked at production in individual oil fields and predicted that the United States would see the peak of its oil production in 1970 or so, and then drop. His prediction largely came true: Oil production went up but did peak in the 1970s, then plummeted. Oil production has recently gone up in the United States a little bit, but it’s still just barely more than half of what it was in its peak in the 1970s. Hubbert also predicted that the global oil market would peak in about 2000, and for a long time he looked very foolish. But it now has basically plateaued. Since 2004, oil production has increased by about 4%, whereas in the 1950s it rose by about 4% every three months. We haven’t hit a peak; oil production around the world is still rising a little bit. It’s certainly not declining, but we do appear to be near a plateau; supply is definitely rising more slowly than demand. Though there’s plenty of oil in the ground, the oil that remains is in smaller fields, further from shore, under lower pressure, and harder to pump out. Water is another resource that is incredibly precious to us. The predominant way in which we use water is through the food that we eat: 70% of the freshwater that humanity uses goes into agriculture. The Ogallala Aquifer, the giant body of freshwater under the surface of the Earth in the Great Plains of the United States, is fossil water left from the melting and the retreat of glaciers in the end of the last Ice Age, 12,000–14,000 years ago. Its refill time is somewhere between 5,000 and 10,000 years from normal rainfall. Since 1960, we’ve drained between a third and a half of the water in this body, depending on what estimate you look at. In some areas, the water table is dropping about three feet per year. If this was a surface lake in the United States or Canada, and people saw that happening, they’d stop it. But because it’s out of sight, it’s just considered a resource that we can tap. And indeed, in the north Texas area, wells are starting to fail already, and farms are being abandoned in some cases, because they can’t get to the water that they once did. Perhaps the largest risk of all is climate change. We’ve increased the temperature of the planet by about 2°F in the last 130 years, and that rate is accelerating. This is primarily because of the carbon dioxide we’ve put into the atmosphere, along with methane and nitrous oxide. CO2 levels, now at over 390 parts per million, are the highest they’ve been in about 15 million years. Ice cores go back at least a million years, and we know that they’re the highest they’ve been in that time. Historically, when CO2 levels are high, temperature is also high. But also, historically, in the lifetime of our species, we’ve actually never existed as human beings while CO2 levels have been this high. For example, glaciers such as the Bear and Pedersen in Alaska have disappeared just since 1920. As these glaciers melt, they produce water that goes into the seas and helps to raise sea levels. Over the next century, the seas are expected to rise about 3 to 6 feet. Most of that actually will not be melting glaciers; it’s thermal expansion: As the ocean gets warmer, it gets a little bit bigger. But 3 to 6 feet over a century doesn’t sound like that big a deal to us, so we think of that as a distant problem. The reality is that there’s a more severe problem with climate change: its impact on the weather and on agriculture. In 2003, Europe went through its worst heat wave since 1540. Ukraine lost 75% of its wheat crop. In 2009, China had a once-in-a-century level drought; in 2010 they had another once-in-a-century level drought. That’s twice. Wells that had given water continuously since the fifteenth century ran dry. When those rains returned, when the water that was soaked up by the atmosphere came back down, it came down on Pakistan, and half of Pakistan was under water in the floods of 2010. An area larger than Germany was under water. Warmer air carries more water. Every degree Celsius that you increase the temperature value of air, it carries 7% more water. But it doesn’t carry that water uniformly. It can suck water away from one place and then deliver it in a deluge in another place. So both the droughts are up and flooding is up simultaneously, as precipitation becomes more lumpy and more concentrated. In Russia’s 2010 heat wave, 55,000 people died, 11,000 of them in Moscow alone. In 2011, the United States had the driest 10-month period ever in the American South, and Texas saw its worst wildfires ever. And 2012 was the worst drought in the United States since the Dust Bowl—the corn crop shrank by 20%. So that’s the big risk the world faces: that radical weather will change how we grow food, which is still our most important energy source—even more important than fossil fuels. A number of people in the environmentalist movement are saying that we have to just stop growing. For instance, in his book Peak Everything: Waking Up to the Century of Declines, Richard Heinberg of the Post-Carbon Institute says that the Earth is full. Get used to it, and get ready for a world where you live with less wealth, and where your children live with less wealth, than any before. I don’t think this idea of stopping growth is realistic, because there are a top billion people who live pretty well and there are another 6 billion who don’t and are hungry for it. We see demand rising for everything—water, food, energy—and that demand is rising not in the United States or Europe or Canada or Australia. It’s rising in the developing world. This is the area that will create all of the increased demand for physical resources. Even if we could, by some chance, say That’s enough, sorry, we’re not going to let you use these resources, which is doubtful, it wouldn’t be just, because the West got rich by using those natural resources. So we need to find a different way. Ideas as a Resource Expander, Resource Preserver, and Waste Reducer The best-selling environmental book of all time, Limits to Growth, was based on computer modeling. It was a simple model with only about eight variables of what would happen in the world. It showed that economic growth, more wealth, would inevitably lead to more pollution and more consumption of finite resources, which would in turn take us beyond the limits and lead ultimately to collapse. While it’s been widely reported recently that its predictions are coming true, that’s actually not the case. If you look at the vast majority of the numbers that the researchers predict in this model, they’re not coming true. Why did they get these things wrong? The most important thing that the forecasters did was underestimate the power of new ideas to expand resources, or to expand wealth while using fewer resources. Ideas have done tremendous things for us. Let’s start with food. In The Population Bomb (1968), Paul Ehrlich predicted that food supply could not support the population, just as Malthus did. But what’s happened is that we’ve doubled population since 1960, and we’ve nearly tripled the food supply in total. We’ve increased by 30%–40% the food supply per person since the 1960s. Let’s look at this on a very long time scale. How many people can you feed with an acre of land? Before the advent of agriculture, an acre of land could feed less than a thousandth of a person. Today it’s about three people, on average, who can be fed by one acre of land. Pre-agriculture, it took 3,000 acres for one person to stay alive through hunting and gathering. With agriculture, that footprint has shrunk from 3,000 acres to one-third of one acre. That’s not because there’s any more sunlight, which is ultimately what food is; it’s because we’ve changed the productivity of the resource by innovation in farming—and then thousands of innovations on top of that to increase it even more. In fact, the reason we have the forests that we have on the planet is because we were able to handle a doubling of the population since 1960 without increasing farmland by more than about 10%. If we had to have doubled our farmland, we would have chopped down all the remaining forests on the planet. Ideas can reduce resource use. I can give you many other examples. In the United States, the amount of energy used on farms per calorie grown has actually dropped by about half since the 1970s. That’s in part because we now only use about a tenth of the energy to create synthetic nitrogen fertilizer, which is an important input. The amount of food that you can grow per drop of water has roughly doubled since the 1980s. In wheat, it’s actually more than tripled since 1960. The amount of water that we use in the United States per person has dropped by about a third since the 1970s, after rising for decades. As agriculture has gotten more efficient, we’re using less water per person. So, again, ideas can reduce resource use. Ideas can also find substitutes for scarce resources. We’re at risk of running out of many things, right? Well, let’s think about some things that have happened in the past. The sperm whale was almost hunted into extinction. Sperm whales were, in the mid-1800s, the best source of illumination. Sperm whale oil—spermaceti—was the premier source of lighting. It burned without smoke, giving a clear, steady light, and the demand for it led to huge hunting of the sperm whales. In a period of about 30 years, we killed off about a third of the sperm whales on the planet. That led to a phenomenon of “peak sperm-whale oil”: The number of sperm whales that the fleet could bring in dropped over time as the sperm whales became more scarce and more afraid of human hunters. Demand rose as supply dropped, and the prices skyrocketed. So it looked a little bit like the situation with oil now. That was solved not by the discovery of more sperm whales, nor by giving up on this thing of lighting. Rather, Abraham Gesner, a Canadian, discovered this thing called kerosene. He found that, if he took coal, heated it up, captured the fumes, and distilled them, he could create this fluid that burned very clear. And he could create it in quantities thousands of times greater than the sperm whales ever could have given up. We have no information suggesting that Gesner was an environmentalist or that he cared about sperm whales at all. He was motivated by scientific curiosity and by the huge business opportunity of going after this lighting market. What he did was dramatically lower the cost of lighting while saving the sperm whales from extinction. One more thing that ideas can do is transform waste into value. In places like Germany and Japan, people are mining landfills. Japan estimates that its landfills alone contain 10-year supplies of gold and rare-earth minerals for the world market. Alcoa estimates that the world’s landfills contain a 15-year supply of aluminum. So there’s tremendous value. When we throw things away, they’re not destroyed. If we “consume” things like aluminum, we’re not really consuming it, we’re rearranging it. We’re changing where it’s located. And in some cases, the concentration of these resources in our landfills is actually higher than it was in our mines. What it takes is energy and technology to get that resource back out and put it back into circulation. Ideas for Stretching the Limits So ideas can reduce resource use, can find substitutes for scarce resources, and can transform waste into value. In that context, what are the limits to growth? Is there a population limit? Yes, there certainly is, but it doesn’t look like we’re going to hit that. Projections right now are that, by the middle of this century, world population will peak between 9 billion and 10 billion, and then start to decline. In fact, we’ll be talking much more about the graying of civilization, and perhaps underpopulation—too-low birthrates on a current trend. What about physical resources? Are there limits to physical resource use on this planet? Absolutely. It really is a finite planet. But where are those limits? To illustrate, let’s start with energy. This is the most important resource that we use, in many ways. But when we consider all the fossil fuels that humanity uses today—all the oil, coal, natural gas, and so on—it pales in comparison to a much larger resource, all around us, which is the amount of energy coming in from our Sun every day. The amount of energy from sunlight that strikes the top of the atmosphere is about 10,000 times as much as the energy that we use from fossil fuels on a daily basis. Ten seconds of sunlight hitting the Earth is as much energy as humanity uses in an entire day; one hour of sunlight hitting the Earth provides as much energy to the planet as a whole as humanity uses from all sources combined in one year. This is an incredibly abundant resource. It manifests in many ways. It heats the atmosphere differentially, creating winds that we can capture for wind power. It evaporates water, which leads to precipitation elsewhere, which turns into things like rivers and waterfalls, which we can capture as hydropower. But by far the largest fraction of it—more than half—is photons hitting the surface of the Earth. Those are so abundant that, with one-third of 1% of the Earth’s land area, using current technology of about 14%-efficient solar cells, we could capture enough electricity to power all of current human needs. The problem is not the abundance of the energy; the problem is cost. Our technology is primitive. Our technology for building solar cells is similar to our technology for manufacturing computer chips. They’re built on silicon wafers in clean rooms at high temperatures, and so they’re very, very expensive. But innovation has been dropping that cost tremendously. Over the last 30 years, we’ve gone from a watt of solar power costing $20 to about $1. That’s a factor of 20. We roughly drop the cost of solar by one-half every decade, more or less. That means that, in the sunniest parts of the world today, solar is now basically at parity in cost, without subsidies, with coal and natural gas. Over the next 12–15 years, that will spread to most of the planet. That’s incredibly good news for us. Of course, we don’t just use energy while the Sun is shining. We use energy at night to power our cities; we use energy in things like vehicles that have to move and that have high energy densities. Both of these need storage, and today’s storage is actually a bigger challenge than capturing energy. But there’s reason to believe that we can tackle the storage problem, as well. For example, consider lithium ion batteries—the batteries that are in your laptop, your cell phone, and so on. The demand to have longer-lasting devices drove tremendous innovations in these batteries in the 1990s and the early part of the 2000s. Between 1991 and 2005, the cost of storage in lithium ion batteries dropped by about a factor of nine, and the density of storage—how much energy you can store in an ounce of battery—increased by a little over double in that time. If we do that again, we would be at the point where grid-scale storage is affordable and we can store that energy overnight. Our electric vehicles have ranges similar to the range you can get in a gasoline-powered vehicle. This is a tall order. This represents perhaps tens of billions of dollars in R&D, but it is something that is possible and for which there is precedent. Another approach being taken is turning energy into fuel. When you use a fuel such as gasoline, it’s not really an energy source. It’s an energy carrier, an energy storage system, if you will. You can store a lot of energy in a very small amount. Today, two pioneers in genome sequencing—Craig Venter and George Church—both have founded companies to create next-generation biofuels. What they’re both leveraging is that gene-sequencing cost is the fastest quantitative area of progress on the planet. What they’re trying to do is engineer microorganisms that consume CO2, sunlight, and sugar and actually excrete fuel as a byproduct. If we could do this, maybe just 1% of the Earth’s surface—or a thirtieth of what we use for agriculture—could provide all the liquid fuels that we need. We would conveniently grow algae on saltwater and waste water, so biofuel production wouldn’t compete for freshwater. And the possible yields are vast if we can get there. If we can crack energy, we can crack everything else: • Water. Water is life. We live in a water world, but only about a tenth of a percent of the water in the world is freshwater that’s accessible to us in some way. Ninety-seven percent of the world’s water is in the oceans and is salty. It used to be that desalination meant boiling water and then catching the steam and letting it condense. Between the times of the ancient Greeks and 1960, desalination technology didn’t really change. But then, it did. People started to create membranes modeled on what cells do, which is allow some things through but not others. They used plastics to force water through and get only the fresh and not the salty. As a result, the amount of energy it takes to desalinate a liter of water has dropped by about a factor of nine in that time. Now, in the world’s largest desalination plants, the price of desalinated water is about a tenth of a cent per gallon. The technology has gotten to the point where it is starting to become a realistic option as an alternative to using up scarce freshwater resources. • Food. Can we grow enough food? Between now and 2050, we have to increase food yield by about 70%. Is that possible? I think it is. In industrialized nations, food yields are already twice what they are in the world as a whole. That’s because we have irrigation, tractors, better pesticides, and so on. Given such energy and wealth, we already know that we can grow enough food to feed the planet. Another option that’s probably cheaper would be to leverage some things that nature’s already produced. What most people don’t know is that the yield of corn per acre and in calories is about 70% higher than the yield of wheat. Corn is a C 4 photosynthesis crop: It uses a different way of turning sunlight and CO2 into sugars that evolved only 30 million years ago. Now, scientists around the world are working on taking these C 4 genes from crops like corn and transplanting them into wheat and rice, which could right away increase the yield of those staple grains by more than 50%. Physical limits do exist, but they are extremely distant. We cannot grow exponentially in our physical resource use forever, but that point is still at least centuries in the future. It’s something we have to address eventually, but it’s not a problem that’s pressing right now. • Wealth. One thing that people don’t appreciate very much is that wealth has been decoupling from physical resource use on this planet. Energy use per capita is going up, CO2 emissions per capita have been going up a little bit, but they are both widely outstripped by the amount of wealth that we’re creating. That’s because we can be more efficient in everything—using less energy per unit of food grown, and so on. This again might sound extremely counterintuitive, but let me give you one concrete example of how that happens. Compare the ENIAC—which in the 1940s was the first digital computer ever created—to an iPhone. An iPhone is billions of times smaller, uses billions of times less energy, and has billions of times more computing power than ENIAC. If you tried to create an iPhone using ENIAC technology, it would be a cube a mile on the side, and it would use more electricity than the state of California. And it wouldn’t have access to the Internet, because you’d have to invent that, as well. This is what I mean when I say ideas are the ultimate resource. The difference between an ENIAC and an iPhone is that the iPhone is embodied knowledge that allows you to do more with less resources. That phenomenon is not limited to high tech. It’s everywhere around us. So ideas are the ultimate resource. They’re the only resource that accumulates over time. Our store of knowledge is actually larger than in the past, as opposed to all physical resources. Challenges Ahead for Innovation Today we are seeing a race between our rate of consumption and our rate of innovation, and there are multiple challenges. One challenge is the Darwinian process, survival of the fittest. In areas like green tech, there will be hundreds and even thousands of companies founded, and 99% of them will go under. That is how innovation happens. The other problem is scale. Just as an example, one of the world’s largest solar arrays is at Nellis Air Force Base in California, and we would need about 10 million of these in order to meet the world’s electricity needs. We have the land, we have the solar energy coming in, but there’s a lot of industrial production that has to happen before we get to that point. Innovation is incredibly powerful, but the pace of innovation compared to the pace of consumption is very important. One thing we can do to increase the pace of innovation is to address the biggest challenge, which is market failure. In 1967, you could stick your hand into the Cuyahoga River, in Ohio, and come up covered in muck and oil. At that time, the river was lined with businesses and factories, and for them the river was a free resource. It was cheaper to pump their waste into the river than it was to pay for disposal at some other sort of facility. The river was a commons that anybody could use or abuse, and the waste they were producing was an externality. To that business or factory, there was no cost to pumping waste into this river. But to the people who depended upon the river, there was a high cost overall. That’s what I mean by a market externality and a market failure, because this was an important resource to all of us. But no one owned it, no one bought or sold it, and so it was treated badly in a way that things with a price are not. That ultimately culminated when, in June 1969, a railway car passing on a bridge threw a spark; the spark hit a slick of oil a mile long on the river, and the river burst into flames. The story made the cover of Time magazine. In many ways, the environmental movement was born of this event as much as it was of Rachel Carson’s Silent Spring. In the following three years, the United States created the Environmental Protection Agency and passed the Clean Water and Clean Air acts. Almost every environmental problem on the planet is an issue of the commons, whether it’s chopping down forests that no one owns, draining lakes that no one owns, using up fish in the ocean that no one owns, or polluting the atmosphere because no one owns it, or heating up the planet. They’re all issues of the commons. They’re all issues where there is no cost to an individual entity to deplete something and no cost to overconsume something, but there is a greater cost that’s externalized and pushed on everybody else who shares this. Now let’s come back again to what Limits to Growth said, which was that economic growth always led to more pollution and more consumption, put us beyond limits, and ends with collapse. So if that’s the case, all those things we just talked about should be getting worse. But as the condition of the Cuyahoga River today illustrates, that is not the case. GDP in the United States is three times what it was when the Cuyahoga River caught on fire, so shouldn’t it be more polluted? It’s not. Instead, it’s the cleanest it’s been in decades. That’s not because we stopped growth. It’s because we made intelligent choices about managing that commons. Another example: In the 1970s, we discovered that the ozone layer was thinning to such an extent that it literally could drive the extinction of all land species on Earth. But it’s actually getting better. It’s turned a corner, it’s improving ahead of schedule, and it’s on track to being the healthiest it’s been in a century. That’s because we’ve reduced the emissions of CFCs, which destroy ozone; we’ve dropped the amount of them that we emit into the atmosphere basically to zero. And yet industry has not ground to a halt because of this, either. Economic growth has not faltered. And one last example: Acid rain—which is primarily produced by sulfur dioxide emitted by coal-burning power plants—is mostly gone as an issue. Emissions of sulfur dioxide are down by about a factor of two. That’s in part because we created a strategy called cap and trade: It capped the amount of SO2 that you could emit, then allowed you to swap and buy emission credits from others to find the optimal way to do that. The cost, interestingly enough, has always been lower than projected. In each of these cases, industry has said, This will end things. Ronald Reagan’s chief of staff said the economy would grind to a halt, and the EPA would come in with lower cost estimates. But the EPA has always been wrong: The EPA cost estimate has always been too high. Analysis of all of these efforts in the past shows that reducing emissions is always cheaper than you expect, but cleaning up the mess afterwards is always more expensive than you’d guess. Today, the biggest commons issue is that of climate change, with the CO2 and other greenhouse gases that we’re pumping into the atmosphere. A logical thing to do would be to put a price on these. If you pollute, if you’re pumping CO2 into the atmosphere and it’s warming the planet, so you’re causing harm to other people in a very diffuse way. Therefore, you should be paying in proportion to that harm you’re doing to offset it. But if we do that, won’t that have a massive impact on the economy? This all relates to energy, which drives a huge fraction of the economy. Manufacturing depends on it. Transport depends on it. So wouldn’t it be a huge problem if we were to actually put a price on these carbon emissions? Well, there has been innovative thinking about that, as well. One thing that economists have always told us is that, if you’re going to tax, tax the bad, not the good. Whatever it is that you tax, you will get less of it. So tax the bad, not the good. The model that would be the ideal for putting a price on pollution is what we call a revenue-neutral model. Revenue-neutral carbon tax, revenue-neutral cap and trade. Let’s model it as a tax: Today, a country makes a certain amount of revenue for its government in income tax, let’s say. If you want to tax pollution, the way to do this without impacting the economy is to increase your pollution tax in the same manner that you decrease the income tax. The government then is capturing the same amount of money from the economy as a whole, so there’s no economic slowdown as a result of this. This has a positive effect on the environment because it tips the scales of price. Now, if you’re shopping for energy, and you’re looking at solar versus coal or natural gas, the carbon price has increased the price of coal and natural gas to you, but not the cost of solar. It shifts customer behavior from one to the other while having no net impact on the economy, and probably a net benefit on the economy in the long run as more investment in green energy drives the price down. Toward a Wealthier, Cleaner Future The number-one thing I want you to take away is that pollution and overconsumption are not inevitable outcomes of growth. While tripling the wealth of North America, for instance, we’ve gone from an ozone layer that was rapidly deteriorating to one that is bouncing back. The fundamental issue is not one of limits to growth; it’s one of the policy we choose, and it’s one of how we structure our economy to value all the things we depend upon and not just those things that are owned privately. What can we do, each of us? Four things: First is to communicate. These issues are divisive, but we know that beliefs and attitudes on issues like this spread word of mouth. They spread person to person, from person you trust to person you trust. So talk about it. Many of us have friends or colleagues or family on the other side of these issues, but talk about it. You’re better able to persuade them than anyone else is. Second is to participate. By that I mean politically. Local governments, state and province governments, and national governments are responsive when they hear from their constituents about these issues. It changes their attitudes. Because so few constituents actually make a call to the office of their legislator, or write a letter, a few can make a very large impact. Third is to innovate. These problems aren’t solved yet. We don’t have the technologies for these problems today. The trend lines look very good, but the next 10 years of those trend lines demand lots of bright people, lots of bright ideas, and lots of R&D. So if you’re thinking about a career change, or if you know any young people trying to figure out what their career is now, these are careers that (A) will be very important to us in the future and (B) will probably be quite lucrative for them.

### 2NC---Uniqueness

#### Tech industry wage inflation is on the brink

Suman Bhattacharyya 22, Wall Street Journal Reporter. April 21, 2022. "Tech Wage Inflation Puts Pressure on Companies" <https://www.wsj.com/articles/tech-wage-inflation-puts-pressure-on-companies-11650533400>

Wage inflation in the technology sector is accelerating, pressuring companies to boost compensation for key roles by 20% or more as they compete for a limited pool of workers skilled in areas such as cloud computing and data science.

There is no single source of data on all tech jobs, but it is clear from a range of market analysts and executives that demand for labor in the tech sector is on the rise. During the first quarter, U.S. employers posted 1.1 million tech jobs, an increase of 43% from a year earlier, according to information technology trade group CompTIA.

Demand for workers to fill those jobs has been surging since the pandemic began, prompting companies to turn to remote work and other digital initiatives. Inflation at a 40-year-high and the war in Ukraine disrupting tech and outsourcing hubs in Europe also are pushing compensation for tech workers higher.

The tech roles in greatest demand include cloud computing architects, data scientists and modelers, and machine learning experts. Staffing firm Mondo, an Addison Group company, said at the high end of the compensation range, cloud architects saw average salary increases of 25% between 2020 and this year, while average salaries for software engineers rose 11% over the same period.

The rising cost of hiring and retaining top tech talent is creating challenges for chief information officers and other tech leaders and has even caught the attention of chief executive officers.

“It’s stunning,” said Michael Burns, co-founder and executive chairman of iDEAL Semiconductor Devices and managing director of the Murray Hill Group venture capital and private-equity firm. Mr. Burns said wage increases in the tech sector can top 20%, and in hot markets such as Austin, Texas, they can hit 30%.

CIOs and other tech chiefs are under pressure to convince board members to approve higher spending for tech salaries that may exceed pay levels for other jobs, according to Scott Spradley, executive vice president and chief technology and automation officer at Tyson Foods Inc. Given the tight labor market, the cost of running and maintaining IT operations is on the rise, and the cost of investing in innovation is going up at an even faster pace, he said.

Wage pressures are acute in Europe, too, according to Vineet Jain, founder and CEO of Egnyte Inc. The enterprise file-sharing company employs 250 people in Poland, where average wage increases are 50% and some workers have doubled their pay during the past year, according to Mr. Jain. “And these were not low-paid people,” he said.

Rising salaries aren’t limited to veteran tech workers. Jai Bhagat, a software engineer at HashiCorp, a San Francisco-based enterprise software company, said some hiring managers in the tech industry are offering recent graduates compensation packages in the six-figure range, compared with starting salaries of $70,000 to $85,000 a few years ago.

Outsize gains in tech compensation, while increasingly common, aren’t universal. An AT&T Inc. spokesperson said in an email that salary increases in the company’s technology services organization averaged 5% this year. Cisco Systems Inc. in an email said average pay levels for its software engineers across the U.S. rose between 5% and 10% this past year.

## Advantage Counterplans

### 1NC---Democracy

#### CP solves authoritarian AI without security cooperation

Andrew Imbrie et al 20, Andrew Imbrie Ryan Fedasiuk Catherine Aiken Tarun Chhabra Husanjot Chahal. Center for Security and Emerging Technology (CSET) at Georgetown’s Walsh School of Foreign Service is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community. February. "Agile Alliances: How the United States and its Allies Can Deliver a Democratic Way of AI" //pipk

One of the chief attractions of Chinese-supplied consumer technologies (5G, cell phones, computers, digital wallets) is that they are less expensive than Western equivalents, and market access is often a condition for Chinese companies investing in developing countries. For example, some allies and partners are reluctant to ban Huawei for fear of losing access to the Chinese market and investments. Even among partners, the appeal of cost effectiveness sometimes outweighs considerations of privacy and security. The CSET survey found that cost effectiveness matters more than privacy for international agreements around software contracts. Yet privacy matters more among partners for international agreements around data storage and sharing. Surveyed officials were split in terms of the relative importance of privacy and cost for international agreements around novel applications and hardware investment. Germany, Australia, and the EU tended to favor privacy in all cases, while Colombia and the Czech Republic tended to favor cost effectiveness when considering international collaboration.

To promote a rules-based global trading order, the United States should not mimic China’s model of state-driven, top-down national development strategies that trade investment for market access. Instead, the United States should form a multilateral consortium to coordinate the extension of credit to European mobile telecommunications networks and invest in next-generation networks.91

The United States and its allies should also launch a multilateral digital infrastructure network. This network could be modeled on USAID’s Higher Education Solutions Network, a partnership between USAID and development labs at seven major universities, and the EU’s Digital4Development policy, an initiative that harnesses information and communications technologies to promote sustainable development.92 A multilateral digital infrastructure network would enable the United States and its allies to partner with developing countries to build digital capacity in support of the UN’s Sustainable Development Goals. The right approach would ensure that digital systems in emerging markets are open, secure, resilient, and interoperable, while empowering developing countries to protect data privacy, meet their domestic needs, and access high-performance computing and mobile internet technologies.

Liberal democratic governments have established frameworks and standards for good governance tied to development lending and giving. Democratic countries should include AI in these frameworks along with capacity building to ensure that developing countries can make sovereign and democratically accountable decisions about the deployment of AI. Many developing countries are growth markets and present opportunities to shape AI governance consistent with liberal democratic principles. As part of this effort, the United States and its allies should integrate federated learning techniques and data privacy into digital capacity building efforts with developing countries. By creating an accelerator fund for privacy-preserving machine learning technologies, the United States and its allies could promote an alternative model of development that puts data protection and privacy at the absolute center.

## AI Center CP

### 1NC---OFF

#### The United States federal government should propose a Artificial Intelligence Center in the North Atlantic Treaty Organization with authority over artificial intelligence military logistics pilot projects

#### The counterplan solves the aff and is competitive---creating an AI center results in effective evaluation procedures and overcomes resistance but ownership is key

Andrea Gilli et al 20, Senior Researcher at the NATO Defense College where he works on issues related to technological change and military innovation. He has been visiting and postdoctoral fellow at Johns Hopkins University and Columbia University as well as Stanford University (where he remains an Affiliate) and Harvard University. Mauro Gilli is a Senior Researcher in Military Technology and International Security at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology, ETHZurich. Before joining CSS, he was a post-doctoral fellow at the Dickey Center, Dartmouth College. Ann-Sophie Leonard is a former Mercator Fellow on International Affairs, focusing on the intersection of international security and technology. She was a Visiting Fellow at the Research Division of the NATO Defense College in Rome from September to December 2019. Zoe Stanley-Lockman is an Associate Research Fellow in the Military Transformations Programme at the Institute of Defence and Strategic Studies at the S. Rajaratnam School of International Studies in Singapore. “NATO-Mation”: Strategies for Leading in the Age of Artificial Intelligence. NDC Research Paper No.15 – December 2020 //pipk

While innovation is often treated and discussed as an outcome, it is in fact also a process whereby champions – whether individuals or organizations – promote and implement changes leading to performance, mission or operational improvement.116 Within NATO, many stakeholders have an inherent interest in AI and in promoting the AI agenda. However, there is no clear “champion” whose goal is to steer the Alliance’s approach to adopting the technology, promoting the necessary reform, and devising the best practices for its employment. For this reason, the process of “NATO-mation” could benefit significantly from a centre specifically intended to serve this goal – tentatively referred to here as an Artificial Intelligence, Integration and Implementation-Enabling Centre (A3IC). Such a centre could lead adoption of AI for the Alliance, support Allies in their own adoption strategies, and connect the relevant offices and institutions at both the national and NATO levels. With a focus on training and interoperability, an AI champion for NATO could ensure that the Alliance treats innovation as an ongoing process and disseminates successful outcomes.

The innovation process often requires a person or an organization mentoring, supervising, advocating and protecting innovations and innovators. Having an innovation champion is important to promote those micro-changes that often permit the successful adoption of an innovation: this is achieved by aligning the interests of all the individuals involved with the overall goal, so that resistance, opposition and sometimes even boycotting are minimized and addressed.117 While the buzzword “innovation” is generally perceived favourably, resistance often emerges because of cultural barriers such as opposition to change, sociological factors such as group identity and concern for loss of status, organizational dynamics such as career advancement being hindered by a new technology, as well as for cognitive and psychological reasons.118 The old adage goes: the thing people really hate, more than the way things are, is change.

Military innovation poses even more subtle challenges. Adoption of AI may be perceived as especially daunting, because the technology is intangible and difficult to quantify: we can neither touch it nor see it. Additionally, previous lessons of military innovations show the close relationship between platforms and service identity. For example, innovation in military aviation became easier when air branches became independent organizations, separate from armies and navies.119 Similarly, operators of transport or rotary-wing aircraft have often struggled to obtain the necessary recognition and resources from within their respective military services. These dynamics also occur between surface and underwater services, as well as between combat and intelligence or between surveillance and reconnaissance units. It remains to be seen where AI will fit into the culture of military organizations, but algorithms, data and processors are unlikely to be in the ensigns of any military service, at least in the foreseeable future: the tense discussions about counting drone operations as flying hours or assigning medals to drone pilots bear testament to that.120 This is a small, but powerful lesson: in the foreseeable future, some military services could lack interest in, or display insufficient attention to, these domains.121 This is why an AI champion within NATO may be particularly important.122

There is an additional consideration: interoperability would be difficult without coordination among Allies. At the NATO level, a centralized body could play a particularly useful and effective role in this respect. Future discussions could determine whether such a Centre should be independent, like a Centre of Excellence, or sit within the NATO Enterprise structure (natural options being under Allied Command Transformation or in the NATO Communications and Information Agency). There are, however, strong reasons to assign such a Centre a number of specific goals.

Lead. The Centre should be at the forefront of NATO’s and the Allies’ AI efforts, including discussions about ethics and ownership of pilot projects (see below) as well as development of targeted solutions to existing problems and challenges.

Support. The A3IC should have an interest in helping Allies adopt AI through a set of procedures, roadmaps, best practices and, where possible, readily available solutions, either developed in-house or borrowed from others. From ethics to training, from recruitment to procurement, from cyber security to data management, the Centre could provide important support, especially for some Allies or some of their services that may lack inhouse solutions or expertise. Cases in point would be Testing and Evaluation (T&E) and Verification and Validation (V&V): with the adoption of ML, these will have to be rethought, upgraded and updated in order to integrate the non-deterministic nature of algorithms into existing procedures and methods.123 Similarly, in the age of software, procurement needs a major upgrade. In contrast to traditional military platforms, it is faced with a paradigm shift: rather than deliver finished and well-functioning products, it must come up with adaptable solutions that, by their very nature, can never be considered as “done” once and for all.124 Realistically, not all Allies possess the necessary expertise to face such challenges. The Centre could play an important role in these areas. Since the AI ecosystem, as this document shows, is admittedly massive but also scalable, for many Allies it may be much more convenient to rely on common, Alliance-wide capabilities, since they would probably struggle to achieve the required depth and the breadth if left to their own devices.

Connect. The Alliance will not be effective if individual Allies’ efforts remain disconnected; and it will be more efficient if Allies are able to build on each other’s progress and achievements. The Centre could play a major role in this respect. For instance, the software community around the world relies on platforms such as GitHub to accelerate software development.125 The Alliance has the opportunity to move in the same direction, enabling Allies to benefit from each other’s progress. Researchers in different fields need the same types of tools, from science workflows to AI-driven experimentation, from testing and evaluation to other domains. If NATO’s A3IC could provide a central repository of AI software, it would connect all the actors, accelerate their work and also address potential failures.126 Similar considerations apply to data. “Usually, the biggest challenges [are] related to getting sufficient high-quality training data”. In fact, “system performance is directly tied to data quantity, quality, and representativeness”.127 For the A3IC, a key goal would be to make training data available, as this would dramatically accelerate Allies’ progress. Recent progress in AI has been possible, because nowadays there are “many open source code libraries and developer tools that allow organizations to use and build upon the work of external communities. As a result, no team or organization has to start from scratch, and may parts that used to require highly specialized expertise have been largely automated”.128 The A3IC could play a similar role in making all tools and tests available. This is particularly important for T&E/V&V activities, as will be discussed later.

Initiate. Building on its own and the Allies’ work, the Centre could identify and then propose solutions to the Allies in order to achieve efficiencies, spread AI fluency and favour interoperability. Innovation is, often, a cognitive or cultural process: individuals and organizations need to know they are lagging behind, inefficient or faced with a problem in order to accelerate, to improve, and to find solutions. The A3IC could approach NATO Allies and promote readily available packages. The package of administrative and military functions discussed earlier, where AI can be plugged in, integrated and exploited, would be beneficial for all Allies.

Train. In order to NATO-mate, Allies’ services and units will have to develop in-house AI teams – not only to support their activities, but also to execute an initial sequence of cross-functional enabling projects for different divisions/business units.129 In this respect, since AI talent – as will be discussed – is scarce and difficult to recruit and retain, AI training is particularly important. The A3IC could play a relevant role in providing it. On the one hand, once AI teams are established, they may in fact better understand how to exploit AI for the purpose of the organization. On the other hand, resistance to AI, due to lack of knowledge, is likely: “People are naturally nervous about something they don’t understand”.130 This is the reason why an “enterprise-wide educational programme to teach everyone about the basics of AI and its benefits for the workplace” could help address some concerns and, overall, reduce scepticism.131 The overall goal is to increase AI literacy within NATO and its Allies, as the US National Security Commission on Artificial Intelligence notes.132 However, it is important to emphasize the required conceptual change: not only have individuals to be able to use new tools, but also they also need to be in a position to take full advantage of them. For instance, in business, “intelligent analysts are used to thinking in probabilities […]. But to make a recommendation for action based on probabilities, they need justifications to build their case […]”. AI platforms help conduct scenario planning and build a case for reacting to a probabilistic event.133

Disseminate. It is also imperative that the AI quotient within the Alliance grows. This goes beyond simple training. Nowadays, every employee in an office is expected to have basic IT literacy. This mostly consists of fluency with MS Windows Office. The same should hold for AI: individuals within NATO and the nations should progressively become fluent with the various packages and opportunities. This does not mean that every operator is expected to code or understand the intricacies of how models function. This is more about user interfaces, solutions, and understanding opportunities and limits. Most people use Facebook, Twitter or Instagram on a daily basis. This does not mean they understand the algorithms and the software integration challenges related to third-party applications. In partnership with the existing educational facilities and institutions within, and outside, the Alliance and the Allies, the Centre could coordinate dissemination efforts – whether as part of outreach or education. The ultimate aim of this would be to equip interested stakeholders with the necessary skills and expertise.

Notwithstanding the important contributions this centre could deliver, it is important to be realistic: challenges will emerge with its inception. Three aspects deserve attention. First, discussions about its hierarchical location within existing structures are necessary, but could slow down its creation or hamper its effectiveness. Second, recruitment could generate tensions among different actors. Were the Centre to be filled with AI experts, some could see it as competing unfairly with national authorities. Conversely, were it to provide just support and coordination, some could see it as less useful and effective. Third, ownership and acceptance may be difficult to secure. Its workforce must necessarily be younger than in most other structures, centres and units. This would mean that, without strong leadership at the top, many could be reluctant to accept its support.

#### Creating new evaluation procedures to measure AI innovations prevents centralization of decision-making

Stefano Costalli 21, Associate Professor of Political Science in the Department of Political and Social Sciences, University of Florence, Italy and Research Fellow of the Michael Nicholson Centre for Conflict and Cooperation, University of Essex. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

First of all, the WG defined the main features of Big Data, which set the terms to evaluate any possible organizational innovation and decision-making method. The first and most apparent characteristic of Big Data is the huge quantity of information available. The high-speed at which the data are generated and need to be processed is another defining factor that needs to be taken into account, in addition to the fact that data will typically be acquired from diverse sources and will have different formats. Moreover, the trustworthiness of the data has to be carefully evaluated, and finally any data can have different value in different phases of the decision-making process. All these features impose specific requirements on organizations that aim at using Big Data to reduce the uncertainty in which they operate. For instance, the huge volume of data compels organizations to acquire new data storage capabilities, while the high-speed demands new processing tools and the variable trustworthiness and value compel organizations to elaborate new methods of analysis. Most importantly, all these innovations must be implemented together, because otherwise the Big Data could not be fruitfully exploited and, on the contrary, could create new problems to the organizations, exposing them to dangerous short circuits.

Considering the available literature and exchanging views among the members of the WG, a general consensus emerged according to which any organization that seeks to exploit Big Data should have clear goals and a well-defined strategy to delineate and implement their specific objectives concerning these tools. This is essential to have a clear understanding of the domains and levels where the organization could profit most from the use of Big Data, which types of data are needed, and what investments will have to be made in order to achieve the organization’s goals. Founding the organization’s decision-making process on the use of Big Data will require important investments, and these have to be guided by a clear strategy. According to the emerging evidence, organizations that invest in Big Data analysis without a clear appraisal of the type of data needed and without carefully defined strategies, are bound to failure, wasting precious resources and possibly ending up in suboptimal situations.

Private companies have adopted diverse organizational structures to work effectively with Big Data, ranging from highly centralized to remarkably decentralized models and including hybrid solutions. However, developing forms of governance that allow the different units of the organization to share data and work together seems fundamental. Before the advent of Big Data, such an approach would have raised problems of information security, and the various units would have been advised to limit data circulation. Conversely, some members of the WG observed that in a Big Data environment, security should be recommended for the outcome of the analysis, not for the data source. Otherwise, organizations would risk obtaining “security through obscurity”. In private companies that use Big Data analysis, no attention is given to individual data, but rather to the overall amount of data, which is the real added value. In any case, while data ownership should not be centralized, the available evidence indicates that data governance should, and the Big Data Analytics (BDA) unit should be carefully located. It needs to be placed where it is most needed, easily accessible by core units, cross-functional and integrated. Relatedly, some members of the WG stressed that a key issue with Big Data is providing decision-makers with data that are truly relevant for their purposes, and not simply interesting.

A key requisite for all organizational innovations to occur and for Big Data analysis to be effective is the development and incorporation of a Big Data culture. Chief data officers and senior data-related leadership positions will acquire crucial importance in the analysis of information and in the actual decision-making process, but these positions require a special mix of talent and tools that are currently scarce in many large organizations, especially in the public sector. The organizations that are implementing big data analysis seem especially in need of ‘translators’ – professionals that can ensure effective communication between the Big Data analysis unit and other parts of the organization, where workers are not data scientist and may not be ready to work directly on complex models. However, organizations willing to use Big Data are also in need of real data scientists and analysts, because sophisticated techniques and data analysis tools eventually rely on talented humans who know how to manage the tools and interpret data. As a result, attracting new types of talented young workers and retaining them creating new career paths and opportunities will represent both an essential organizational innovation and an important challenge.

In fact, some members of the WG highlighted that it will not even be easy to find many workers with the appropriate knowledge and skills to perform the new tasks in old and complex organizations. It is possible to find computer scientists, but sometimes these individuals do not seem to fit well with large organizations whose main core business has not much to do with computer science. At the moment, it is even more difficult to find translators, since in principle these workers should be social scientists with an expertise in Big Data analysis, but most academic institutions are not ready to forge these profiles. For what concerns NATO and national armed forces, this educational task is not even performed by military academies, even though some experiments are emerging. The ideal profile would include technical awareness, quantitative analytical skills, broad vision, flexibility and open-mindedness – and this explains why it is not easy to produce it.

After having analyzed the main organizational innovations NATO will have to take into account in the age of Big Data, the WG tried to identify the main challenges. Most of these challenges are strictly linked to the organizational innovations mentioned above, representing the other side of the coin, as in the case of finding and retaining talented workers with new professional profiles.

The first challenge is embodied by an emerging tension between centralization and decentralization of the decision-making process of organizations that are introducing Big Data analysis in their work. As stressed by various members of the WG, a key issue in the use of Big Data for decision-making is that the data, once analyzed, need to reach critical decision-making levels, and not only (or simply) the top level. Nonetheless, it is apparently quite difficult to translate this principle into concrete organizational forms and procedures. Paradoxically, while Big Data should promote widespread responsibility and tactical awareness, at the moment advanced digitalization seems to be linked to clear centripetal forces in large organizations. So far, technologies such as remote-controlled arms systems and intelligence activities based on real-time data collection have produced strong incentives to micromanagement and to a re-centralization of decisionmaking in military organizations that have implemented these tools. As a matter of fact, these technologies are managed from the center of the command structure, and provide higher ranks with an increased possibility to control their subordinates as well as the expectation of increasing such control with the adoption of additional technologies. This powerful tendency risks to threaten initiative and reduce the flexibility of military organizations, decreasing their overall capacity to learn and adapt. While the full exploitation of Big Data and the optimization of their use would require the information to reach the most relevant levels, the centripetal tendency leads towards the de-responsibilization of the lower ranks on the ground and to a progressive loss of practice in choosing. This process is not only inefficient for the reasons mentioned above, but also potentially dangerous because Big Data do not fully eliminate uncertainty: in specific occasions, the data can be inaccurate or not available due to technical problems and, in these cases, the personnel on the ground has to be ready to adapt and react basing their decisions on their experience. Thus, various members of the WG recommended NATO to integrate Big Data in the organization’s decisionmaking, favoring diffused ownership and devising different tools for different branches of the organization, based on their specificities. The implementation of Big Data can and should be used to increase flexibility, situational awareness and action in accordance with the center’s intent but without centralizing all decisions and producing the illusion of complete control.

Some members of the WG suggested that it is crucial for NATO – and for all big organizations engaged in the use of Big Data – to create well-designed and reliable evaluation procedures to measure the effectiveness of organizational innovations as well as of the execution of the new decision-making processes. Identifying the initial failures is especially important, to learn from them and avoid structural problems. This issue is linked to other potential challenges highlighted during the discussions of the WG. For instance, some members pointed out that when adopting Big Data, certain member countries will probably do better than others, and this could cause problems of interoperability, but also learning opportunities. Finally, a well-designed evaluation system will also help avoid some deep risks that automated decision-making could represent for the values of NATO. In fact, some members of the WG stressed that what distinguishes democracies from authoritarian regimes or tech dystopias run by robots is that, ultimately, citizens make the rules that have to be implemented. Moving towards automated decision-making as a result of Big Data analysis in matters of war and peace, life and death, is extremely risky, and the implementation of Big Data cannot decrease human control and responsibilities. Some of NATO’s authoritarian adversaries are already facing smaller legal and normative obstacles in the use of Big Data, but NATO will have to carefully check the impact of next generation’s technologies on the democratic values and legal frameworks of its members.

Conclusion The availability of Big Data is promising to revolutionize the business of private companies, the work of public administration and the bases of decision-making in military organizations. The possibility to collect immense dataset on multiple dimensions on reality and update them constantly and in real time could greatly reduce the uncertainty that dominates many environments, including military affairs and actual combat operations.

However, organizations that aim at exploiting this possibility effectively will have to change their governance and their operational procedures substantially. For this reason, WG1 started its works reviewing the available knowledge on the organizational innovations required, seeking to identify useful lessons for NATO. Subsequently, WG1 tried to detect possible organizational challenges for NATO as a result of the Big Data revolution, suggesting ways to tackle them.

First of all, any organization willing to exploit Big Data must have clear goals and strategies to implement their objectives concerning Big Data. This is essential to produce a clear assessment of the areas and levels where the organization could profit most from the introduction of Big Data analysis. As a matter of fact, it is crucial to understand that, in order to be fully effective, the information collected through Big Data needs to reach the points where it is more relevant. Moreover, a key requisite for all organizational innovations to take place and produce results, is the development of a Big Data culture. The new positions will require special talents and expertise that are currently scarce in many military organizations. WG1 highlighted that it will not be easy to attract these talents and retain them in military organizations, if not by creating new career paths and opportunities.

As regards the main organizational challenges, the members of WG1 found that a major challenge is represented by an emerging tension between centralization and decentralization of the decision-making process in military organizations that are introducing Big Data analysis in their work. Somehow paradoxically, while Big Data should promote widespread responsibility and tactical awareness, at the moment advanced digitalization seems to be linked to clear centripetal forces in large organizations. This is not an inevitable path – flexibility and shared ownership of information are compatible with the introduction of Big Data, but big organizations have to be aware of this tension and set up evaluation systems to control the effectiveness of the innovations adopted.

#### Centralization turns the case---now is the key time to shape digital policy to protect Mission Control doctrine

Paolo Spagnoletti & Andrea Salvi 21,. Associate Professor of Information Systems and Organization, Luiss Business School. Postdoctoral Research Fellow at the Department of Business and Management at LUISS. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

This chapter looks at Mission Command as a manifestation of collective mindfulness for HROs. Mission Command (Auftragstaktik) is a doctrine born to address these environmental constraints through diffused leadership to attain strategic objectives set by the higher ranks. In other words, in a Mission Command framework, the goal is identified and indicated at the top of the command chain – how to reach said goal is delegated to lower ranks and to specialists. Decisions in this context are a by-product of a thorough situational analysis that encompasses evidence from the battlefield, condensed in tactical decisions and abiding the strategic address laid out by high-rank decision makers. Such a course of action requires high levels of cooperation and trust at multiple levels. In first place, lower units – at all levels – need to be aware of the strategic goals set by the commanding officers and – most importantly – they need to embrace and share their rationale. Secondly, horizontal coordination is required: the operating units need to trust each other. Thirdly, lower officers need to fully embrace the logic of mission command and take initiative to accomplish the mission.

Such doctrine is in stark contrast with the so-called “managerial approach” adamantly adopted and renown among the ranks of the US Army almost until the Vietnam War (Shamir, 2010). The latter was heavily reliant on traditional “business oriented techniques”: decisions were taken from above, making use of large volumes of data. As Shamir (2010: 649) puts it: “the managerial approach is characterized by centralization, standardization, detailed planning quantitative analysis and aspires for maximum efficiency and certainty”. In other words, the command chain promoted and enforced a purely vertical doctrine of command, rewarding compliance with meticulously detailed orders and discouraging deviance from the established pathway.

Starting from the eighties, both the British and American Army progressively turned into a more decentralized philosophy of command (Farrell, 2008; Shamir, 2011), better suited ”to contend with the demands, uncertainties and frictions of command in war” (Yardley & Kakabadse, 2007; British Army, 1995). Said management methodology has been codified in doctrinal documents (see e.g. US Department of the Army, 2014; NATO, 2010; UK MoD, 2014), and most military organizations have adapted to it and took measures to implement it in manoeuvre warfare. These measures include extensive training and leadership programs as well as renewed tactical practices. Empirical and anecdotal evidence suggests that Mission Command increases operative efficacy (Yardley & Kakabadse, 2007). Moreover, it fosters widespread engagement and diffused ownership. Given that “no plan survives the first contact with the enemy” (Hughes, 1995), flexibility and freedom of action are values to be actively pursued: “This requires understanding your superior commanders’ intentions, flexibility of mind, rapid decision-making, good organisation and good communications” (UK MoD, 2014: 31). Despite this promise of success, the literature argues that modern military theory is grounded on Mission Command, but the extent to which extent it has been implemented at various levels is rather unclear (Shamir, 2010).

Yet, the growing use and the organizational implementations of real-time control system technologies have led to the renaissance of direct supervision and micro-management practices (Storr, 2003). Given the availability of fine-grained and detailed data, commanders have an incentive to centralize the decisionmaking process pushing towards a more task-oriented approach. The new wave of digitalization has brought cutting-edge remote-controlled technologies, automatic arms systems and data analytics tools that have seen a widespread application in modern warfare and in recent campaigns. High-rank officers can de-facto monitor and control the battlefield from afar, providing platoons with real-time orders. This approach led to the resurgence of Command and Control (C2), deemed a re-emergent doctrine mainly in Western and technology-intensive armies (Connor, 2002). In principle, these systems are able to provide commanders with clear insights from the operative ground and with a level of “intimacy previously reserved for the men in the trenches” (Shamir, 2011: 166). As a result, according to the critics of this system, flexibility and initiative will be hampered with the result of a progressive de-responsibilization of subordinates (Bateman, 1996). Thus, digitalization seems to be intrinsically in contrast with Mission Command, as “C2 leaders” would be prone to establish a more direct control over the structure. This is problematic for the entire command pyramid: “remote commanders” are less likely be warranted trust from the lower ranks.

This chapter conceptualizes the tension between the centripetal force of digitalization and the diffused leadership underlying Mission Command. It critically reviews the main contributions in the field and concludes that digital tools may be shaped in such a way to favor Mission Command, instead of contrasting its core principles. In other words, Big Data, and other advanced data-driven coordination tools, can be used as means to foster widespread responsibility and tactical awareness in extreme contexts. Therefore, the goal of the analysis is to discuss affordances and constraints of digitalization in command and control of military operations.

The first part of this chapter reviews the concept of Mission Command and presents evidence of its applications and adaptations in contemporary military organizations. The second part will discuss the limits of Mission Command vis-a-vis the digitalization. Furthermore, the study will present the main feature of the C2 approach that supposedly better fit a digitized army. Lastly, it will evaluate the co-existence of digital tools and Mission Command exploring avenues for a balancing stance. This work aims to make a contribution to the field of organizational studies and to that of military studies. It constitutes the first step of a broader project that will test the authors’ claim, empirically resorting to interviews and focus-groups.

### 2NC---Solvency

#### CP solves centralization---identifying early failures is key, which means perm can’t solve

Sonia Lucarelli et al 21. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

Digital revolution has substantially transformed the world we live in, providing great opportunities but also making societies more vulnerable. Technology makes external interferences cheaper, faster and allencompassing: citizens can potentially become direct targets of information warfare, all members of a society can be part of conflicts one way or another. From advanced weaponry to command and control, most security-related domains are undergoing deep transformations as data availability and transmission increase exponentially. In this context, three interconnected aspects are explore through this publication with a view to the Alliance’s evolution: Big Data and organizational challenges for NATO; hybrid threats to Allies’ decisionmaking; the adoption of AI in the defense domain and NATO’s role.

Big Data and Organizational Challenges for NATO. Basing decisions on a much larger amount of information than was previously possible could lead to a real revolution in the decision-making processes of complex organizations, especially because this information would concern different dimensions of reality and it would be constantly updated. Beside the huge quantity of information available, the high speed at which the data are generated and need to be processed is another defining factor of Big Data. Also, they will typically be acquired from diverse sources and their trustworthiness has to be carefully evaluated. Finally, any data can have different value in different phases of the decision-making process. All these features impose specific requirements on organizations that aim at using Big Data to reduce the uncertainty in which they operate. For instance, the huge volume of data compels to acquire new data storage technologies, while the high speed demands new processing tools and the variable trustworthiness and value force organizations to elaborate new methods of analysis. Accordingly, any actor that seeks to exploit Big Data should have clear goals and a well-defined strategy to delineate and implement its specific objectives.

A key issue with Big Data is providing decision makers with data that are truly relevant for their purposes, and not simply interesting. Chief data officers and senior data-related leadership positions will acquire a crucial importance in the analysis of information and in the actual decision-making process, but these positions require a special mix of talent and tools that are currently scarce in many large organizations, especially in the public sector and even more in the military one.

Another key issue lies in the emerging tension between centralization and decentralization of the decisionmaking process of organizations that are introducing Big Data analysis in their work. Paradoxically, while Big Data should promote widespread responsibility and tactical awareness, at the moment advanced digitalization seems to be linked to clear centripetal forces in large organizations. The centripetal tendency leads towards the de-responsibilization of the lower ranks and to a progressive loss of practice in choosing. Thus, it would be advisable to integrate Big Data in the Alliance’s decision-making favoring diffused ownership and devising different tools for different branches of the organization, based on their specificities. It would also be helpful to create well-designed and reliable evaluation procedures to measure the effectiveness of organizational innovations as well as of the execution of the new decision-making processes. In particular, identifying the initial failures is especially important, to learn from them and avoid structural problems.

### 2NC---Centralization Link Wall

#### Situational awareness is key to Mission Command effectiveness---solves successful execution of broader strategy

Paolo Spagnoletti & Andrea Salvi 21,. Associate Professor of Information Systems and Organization, Luiss Business School. Postdoctoral Research Fellow at the Department of Business and Management at LUISS. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

Yet, the application of Mission Command requires a shared understanding of the ‘why’ behind any given operation. Once the strategic objectives – or the ‘commanders’ intent’ – is known, diffused leadership is used to circumvent environmental constraints, seize the momentum and obtain a favorable outcome. This course of action is grounded on high levels of trust. More specifically, subordinates – at all levels – need to be aware of the strategic goals set by the commanding officers and – most importantly – they need to embrace and share their rationale. Secondly, horizontal balance is required: the operating units need to trust each other. Thirdly, lower officers need to fully embrace the logic of mission command and take initiative to accomplish the objectives. How to achieve such unity then? As Yardley, Kakabadse and Neal (2012: 74) note, “the glue that holds mission command together is the culture and values of the organization”. The latter is the catalyst for trust that is fully realized through Mission Command.

Another crucial element of Mission Command is situational awareness. Delegating tactical decision to subordinates requires them to responsibly take ownership of actions and choices on the field to execute the mission and maximize the outcome in accordance to the superiors’ intent. Similarly to what recent works on coordination of first-responders suggest (Wolbers et al., 2018), specialists need to act with relative independence to achieve broader cooperation. Specific knowledge is thus a key factor to allow them to take informed decisions. The work of Bungay (2005) and Yardley and Kakabadse (2007) in particular, illustrate the decay curve of a plan’s effectiveness over time, illustrating the concept presented.

In a neutral scenario, a plan developed through Mission Command decays in a slower way if compared to a vertically-imposed course of action. The reason for that is that Mission Command makes plans that are more flexible and fluid. Yet, as time passes, even Mission Command suffers from loss of effectiveness when situational awareness is not present. That is, even a flexible plan flickers when the operative conditions on the field change: a plan developed at t0 will inevitably not be as effective at t1 and even less so at t2. Conversely, the presence of situational awareness allows to organize a more agile Mission Command. The vertically-imposed plan will perform exactly as in the previous case, since it is not possible to update it ‘spot on’. A second vertically-imposed plan can be developed, but it will inevitably decay over time when conditions change. Instead, Mission Command – in a space of situational awareness – enables the actors to adapt the plan over time, correcting for contingencies and striving for the ‘higher intent’ as conditions change.

Due to this peculiar feature of Mission Command, several authors have analyzed its feasibility as an organizational theory for businesses and the private sector (Pech & Durden, 2003; Yardley et al., 2012; Yardley & Kakabadse, 2007). This approach might be helpful to better equip private actors against contingencies and unexpected threats. As Yardley and Kakabadse (2007: 76) argue, “competitive advantage is often to be found in narrow margins and innovative solutions rapidly developed and brought to market”. Accordingly – as per the military counterpart – leaders should be trained to what the literature defines as “controlled risk-taking” and wide-spread empowerment.5

All in all, Mission Command is one of the most though-provoking organizational doctrines, and provides a viable solution to respond to contemporary security threats.

#### Digitalization threatens mission command---CP solves

Paolo Spagnoletti & Andrea Salvi 21,. Associate Professor of Information Systems and Organization, Luiss Business School. Postdoctoral Research Fellow at the Department of Business and Management at LUISS. “NATO Decision-Making in the Age of Big Data and Artificial Intelligence” Editors: Sonia Lucarelli; Alessandro Marrone; and Francesco Niccolò Moro. Sonia Lucarelli is Professor of International Relations and European Security at the University of Bologna, and member of the Board of Directors of the Istituto Affari Internazionali (IAI). Alessandro Marrone is Head of the Defence Programme of IAI and teaches at the Istituto Superiore di Stato Maggiore Interforze (ISSMI) of the Italian Ministry of Defence. Francesco N. Moro is Associate Professor of Political Science at the University of Bologna and Adjunct Professor of International Relations at the Johns Hopkins University Europe Campus. This publication is the result of the Conference “NATO Decision-making: promises and perils of the Big Data age”, organized by NATO Allied Command Transformation (ACT), the University of Bologna and Istituto Affari Internazionali (IAI) of Rome. <https://www.iai.it/sites/default/files/978195445000.pdf> //pipk

As recounted in the previous section, the debacle in the Vietnam War posited the need for a change, and Mission Command slowly gained prevalence. Nonetheless, digitalization posits several challenges to this doctrine. Remote-controlled technologies as well as automatic arms systems and real-time data intelligence have been seeing a widespread application in military organizations. These devices and techniques provide higher ranks with a virtually unlimited control over their subordinates. Being able to see, hear and evaluate what a platoon experiences, commanders may have an incentive to give tactical directions transcending the original intent-setter role. The archetypal scenario would be that of a circle of officers sitting in a controlroom, overseeing and leading a unit on the other side of the globe. As an anecdotal example, in 2011, during Operation Neptune Spear that led to the killing of Osama bin Laden, the President of the United States was able to receive live updates from the battlefield in the White House Situation Room. The risk – or the promise – is that of a renaissance of micromanagement (Storr, 2003). This approach has brought some authors to announce the re-emergence of a C2 doctrine typical of technology-intensive armies (Connor, 2002). This is further reinforced by the widespread use of semi-automated firepower: drones and tele-guided artillery strikes have become a frequent complement to the activity of soldiers. Despite their effectiveness, these tools are managed from the center of the command structure and risk to eliminate the discretion of soldiers on the ground to decide when and where to use them based on sheer necessity. As mentioned in the introduction, technological advancements provide high officers with more intimacy, with the battlefield tempting them to “impose their preferences on tactical units” (Augier et al., 2014: 1430).

This is inherently a risk for the Mission Command model. The centripetal effect of this technologies may hamper initiative and frustrate flexibility. As Augier et al. (2014) argue, changes brought by the implementation of technological systems may have consequences on an organization’s ability to learn and adapt. In turn, subordinates will have an incentive towards de-responsibilization (Bateman, 1996).

While this is not an automatic process, the lack of ‘practice in choosing’ may lead to a progressive desensitization to contingency. Furthermore, the introduction of these new technologies does not entirely dissolve the risk of the fog of war. As it was outlined in the very opening of this piece, uncertainty is hardly eliminated from a ‘boots on the ground’ scenario. Data may be inaccurate or discontinued due to technical issues: in that case, the cost in human capital may be conspicuous. It follows that “if the confidence of senior leaders outpaces the efficacy of the technology” (Augier et al., 2014: 1430), the space for tactical adaptation may be severely reduced.

In other words, taking away the power to make decisions from the operational level inevitably decreases situational awareness. In turn, as shown in the figures above, this will impact the plans’ effectiveness in the long-run, in cases whereby the flow of information is interrupted or erroneous. Furthermore, this approach makes trust harder to establish, as servicemen would be asked to follow vertically-imposed orders. Empirical examples of this phenomenon include the implementation of the Below-Blue Force Tracker (BFT). Among other functions, it provides the command center with the GPS coordinates and real-time tracking of the movements of troops. The original rationale behind this system is allowing a more agile manoeuvring at the tactical level, vis-à-vis the fine-grained disaggregated data. Conversely, the command center can use the aggregated data to provide units with strategic directions (Augier et al., 2014). The estimated marginal effect of its implementation translated in a reduction of Blue-on-Blue events between 24% and 12% in the Gulf War, increasing situational awareness of commanders not only towards enemy forces, but especially towards movement of allied ones (Augier et al., 2014).

Yet, having more trust in technology than in the lower levels of the organization is highly problematic. In 2003, General Franks of the United States Central Command (CENTCOM) made use of BFT to push forward idled units that did not adopt an aggressive advancement as seen fit to higher strategic goals (Gordon & Trainor, 2006). Furthermore, empirical evidence from surveys suggest that most of the times BFT was used to issue direct orders from the headquarters to Marine platoon commanders, with a progressive centralization of the tactical decision-making (Dreier & Birgl, 2010).

Digitalization and Fragmented Coordination in Military Operations The review of previous studies on data technology in military operations sheds light on the tensions between the centripetal force of digitalization and the diffused leadership principle underlying Mission Command. It is then possible to conclude that digital tools may be shaped in such a way to favor Mission Command, instead of contrasting its core principles. In other words, Big Data, and other advanced data-driven coordination tools, can be used as means to foster widespread responsibility and tactical awareness in extreme contexts. Technical advancements can be used to better support coordination in Mission Command, and do not intrinsically threat the applicability of the doctrine. This chapter thus claims that digitization does not automatically imply a C2 structure. The implementation of new technologies should be adapted to the decentralized nature of a Mission Command environment. A catch-all product indeed has a centripetal effect, while a carefully tailored one may be able to foster diffused ownership. Equipping different branches of the organization with ad hoc tools based on their operative needs and requirements would further their capacity to take initiative, increase situational awareness and act in accordance with the commanders’ intent.

This analysis shows how C2 decisions are embedded in the institutional context of military operations, and highlights affordances and constraints of digital technologies in this specific domain (Orlikowski & Barley, 2001). Since fragmentation has been recognized as a suitable coordination mode in the fast-paced environment of extreme contexts (Wolbers et al., 2018), this chapter claims that combat units in military organizations can achieve flexibility, sensitivity to operations, and improvisation by designing C2 systems that support fragmentation more than integration. By focusing on digital technologies’ role in supporting working around procedures, task delegation, and expertise, further studies can develop a design theory for digital tools effectively supporting the fragmentation paradigm (Wolbers et al., 2018).

In addition to fragmentation in coordination, the present study suggests looking into other affordances of data technologies, such as those emerging in their application to training and simulations tools. Military organizations operate under special conditions characterized by extreme events with a high potential magnitude of consequences for both organizational members and often hostile and non-hostile actors at risk. As military organizations engage in extreme events less frequently than other organizations (e.g. trauma organizations), they may require more extensive collective training and simulations. Due to chance of casualties, such training requires redundancies and cross-functional exercises to ensure flexible job rotation and contingency-driven substitutions. In military organizations, since they often operate under austere conditions or time constraints do not allow personnel replacements, team members must be ready to step up and take the role of other team members, or assume formal leadership positions if leaders are lost. This requires a balance between generalization and specialization – necessitating advanced training and simulations tools for leader-development across combat units. Therefore, future studies can apply a contingency approach to investigate the fit between data technologies and leadership development in extreme contexts (Hannah et al., 2009).

Finally, this study revitalizes the long-standing centralization and decentralization debate in organization studies (Bloomfield & Coombs, 1992), revising it in light of new digital trends. The analysis instantiates the contradiction between data-processing capabilities seen as both centralized hierarchical control systems and as decentralized internal control and interfaces supporting semi-autonomous units. Further empirical investigations on the mechanisms and conditions under which Big Data capabilities can lead to organizational performance in extreme contexts can contribute to work through this dilemma (Mikalef et al., 2018 and 2020).