# SDI Starter Packet --- Cyber Info Sharing Neg

# \*\*On-case\*\*

## A2: Resilience

### 1NC --- Sharing Sufficient

#### Sharing high now

Maigre 22 --- Merle Maigre, Senior Expert on Cyber Security at the e-Governance Academy (eGA), a non-profit think tank that specializes in empowering central and local governments to lead digital transformation programmes and create smart, sustainable and effective e-government, e-democracy and cyber security solutions, “NATO’s Role in Global Cyber Security”, German Marshall Fund, APRIL 06, 2022, https://www.gmfus.org/news/natos-role-global-cyber-security

Attribution is only as good as the information that allies are willing to share. NATO’s value can be in becoming the preferred platform for sharing cyber information. General Paul Nakasone, who heads US Cyber Command, told the House Armed Services subcommittee on intelligence that “in 35 years” he has never seen a better sharing of accurate, timely, and actionable intelligence than what has transpired with Ukraine.30 Sharing information and intelligence with allies “builds coalitions” and can “shine a light on disinformation” campaigns, like the one Russia used to lay the groundwork for their invasion of Ukraine.

### Ext --- Sharing Sufficient

#### NATO sharing intelligence now

CERULUS 22 --- LAURENS CERULUS, Politico, “NATO steps up intelligence-sharing ‘in preparation’ for Russian cyberattacks”, March 24, 2022, <https://www.politico.eu/article/nato-steps-up-intelligence-sharing-in-preparation-of-russian-cyberattacks/>

Leaders of the NATO defense alliance Thursday said they were stepping up intelligence-sharing on feared Russian cyberattacks, following U.S. warnings that Moscow was preparing large-scale attacks on NATO countries linked to its military invasion in Ukraine.

"In preparation for any Russian malicious cyber response to the actions we have taken, we are taking steps to increase the resilience of the infrastructure in our respective nations by strengthening our coordinated cyber defences and improving our shared awareness of cyber threats," said a statement released after NATO leaders met in Brussels Thursday.

U.S. President Joe Biden earlier this week warned that he had "evolving intelligence" that showed Russia was preparing to conduct cyberattacks on U.S. infrastructure, urging organizations in the U.S. to patch their systems in anticipation of attacks. Biden's message added urgency to repeated calls of authorities in NATO countries to prepare for cyberattacks.

NATO leaders also said that "we will continue efforts to support Ukraine in defending its networks against cyber incidents."

### 1NC --- Top Level Cyber D

**No cyber impact**

--- Defenders advantage nullifies any ROI --- assumes NC3 and Infrastructure

**Borghard & Saltzman 19** --- Erica D. Borghard, Adjunct Research Scholar in the Saltzman Institute of War and Peace Studies and an Adjunct Associate Professor in the School of International and Public Affairs, and Shawn W. Lonergan, Senior Advisor to the U.S. Cyberspace Solarium Commission, Strategic Studies Quarterly , Vol. 13, No. 3 (FALL 2019), pp. 122-145, https://www.jstor.org/stable/26760131?seq=1#metadata\_info\_tab\_contents

Therefore, the time and resource requirements to gain access and develop specific offensive capabilities may render important escalatory response options **infeasible or impractical** at the desired time. Operational planning and execution must consider that a given capability **may not** be usable or **even exist** at a chosen time of employment.29 As the above discussion illustrates, many of the target sets that would represent strategic (and therefore escalatory) targets, such as a state’s critical infrastructure or nuclear command and control, **demand extensive planning, pre-positioning, and capability development** in advance of employing offensive capabilities. Therefore, the timing of a crisis plays a crucial role in decisions about cyber escalation responses. Specifically, the time required to develop access to hold strategic targets at risk means that, even if a state seeks to escalate against an adversary using cyber means, it may find itself limited by the accesses and capabilities it possesses **at the moment** a crisis occurs. Cyber response options may be limited to **less decisive** or more vulnerable **target sets**, rather than those that are more strategically significant.

Third, these limitations become even more salient when we consider how strategic interactions are likely to play out over time during repeated crisis interactions. Because the virtual domain is changeable in a way that the physical world is not, actions taken by defenders in the context of a crisis can **radically and unpredictably** alter an attacker’s ability to deliver and sustain effects against a target over time.30 Access and capabilities are **neither guaranteed nor indefinite**—they have a shelf life.31 Footholds into a target’s network that were time intensive to develop **can unexpectedly disappear** as vulnerabilities in a network are patched. Exploits may have a short shelf life as revealing information about them enables targets to identify indicators of compromise (IOCs) and use these to prevent further damage from specific malware strains or quarantine malicious traffic using known malware signatures. An example of the latter is the US Cyber Command initiative, beginning in 2018, to share information about adversary malware by uploading samples to VirusTotal.32 Therefore, a target can “transition from vulnerability (to a particular attack) to invulnerability in, **literally, minutes**.”33 Third-party disclosure about software vulnerabilities by governments or private actors can also unintentionally precipitate the loss of access as exposure about vulnerability information enables network defenders to take measures to remedy them.34 For instance, the disclosures that began in 2016 by the group Shadow Brokers of purportedly pilfered US National Security Agency exploits and zero days ostensibly put US government accesses at risk.35 Put simply, a vulnerability upon which an access relies may in theory be only one update or disclosure away from being patched.

Thus, in the context of an ongoing crisis interaction between an attacker and defender, the former’s operational tempo is likely to be interrupted by the latter’s behavior, forcing the attacker to devote additional time to find or acquire new vulnerabilities and exploits in the midst of an offensive operation or campaign. As Inglis notes, to succeed in an offensive cyber campaign that unfolds over time, attackers must be able to sustain “the efficacy of tools under varying conditions caused by the defender’s response and the natural variability and dynamism of cyberspace.”36 The ability to build or acquire new accesses and capabilities “in real time” during a crisis is highly limited.37 Indeed, General Paul Nakasone remarked in a January 2019 interview on the radical difference in shelf life between conventional and cyber capabilities:

Compare the air and cyberspace domains. Weapons like JDAMs [ Joint Direct Attack Munitions] are an important armament for air operations. How long are those JDAMs good for? Perhaps 5, 10, or 15 years, sometimes longer given the adversary. When we buy a capability or tool for cyberspace . . . we rarely get a prolonged use we can measure in years. Our capabilities rarely last 6 months, let alone 6 years. This is a big difference in two important domains of future conflict.38

Therefore, as a 2013 Defense Science Board report notes, “offensive cyber will always be a **fragile capability**” when pitted against network defenders who are “**continuously improving** network defensive tools and techniques.”39

Each side can take defensive measures to blunt the impact and effectiveness of the other’s access and capabilities—particularly as information about them is revealed. Consequently, strategic accesses and capabilities are likely to become more vulnerable and less reliable over time, shrinking the set of cyber escalatory response options for all parties. This cycle is likely to generate temporal breaks in the pace of adversarial engagements in cyberspace, where states must regroup and develop or rebuild accesses and capabilities during an ongoing interaction. These pauses are likely to diffuse the pressure that typically accompanies—even defines—crisis situations, creating breathing space and, by extension, room for decisionmakers to deliberate alternative courses of action, for domestic political tensions to cool down, for intent to be communicated to adversaries, and for **de-escalation pathways to be determined.**

#### It’s exaggerated and no escalation

Jasmine Rodet 18, Master’s Degree in Cyber Security, Strategy, and Diplomacy from the University of New South Wales, Cyber Security Program Manager at Fortescue Metals Group, “The Threat of Cyber War is Exaggerated”, 11/11/2018, linkedin.com/pulse/threat-cyber-war-exaggerated-jasmine-rodet/

For the regular person on the street, the term ‘cyber war’ is more likely to bring to mind the 1983 movie “WarGames” and the doomsday articles that appear regularly in the media about the ‘cyber battlefield’ and an impending World War III. This essay argues that the threat of cyber war is exaggerated and although it can, by definition, be stated that we are already in a state of cyber war, the impact on states is negligible compared to conventional war domains. The argument is presented in 3 steps. The first step is to define cyber war and cyber weapons, referencing scholars and experts in the area of conventional war and the cyber domain. The second step is to explore who has been exaggerating the threat of cyber war and what their motivations might be. The third is to explore the evidence and quantify the probability and impact that cyberwar has had on states to date. ‘Cyber war’ is a term often used interchangeably in media with cyber-crime, cyber-attacks, cyber-conflict and cyber-incidents, creating confusion amongst the public and scholars alike. Clausewitz (1989, 75), in his book, On War, defines war as ‘an act of force to compel the enemy to do our will’. Rid (2012, 7) on the other interprets Clausewitz use of ‘force’ as meaning ‘violent’ force. According to Rid, if an act is not potentially violent, it is not an act of war. However, Stone (2013, 107) describes ‘cyber war’ as a politically motivated act of force, not necessarily lethal and not necessarily attributable. The definition by Powers and Jablonski states more simply that cyber war is the utilisation of digital networks for geopolitical purposes (Nocetti 2016, 464). Neither of the latter two definitions requires violence to qualify as cyber war. Under these definitions, the Stuxnet cyber-incident in 2010 and the Estonia incident in 2007 would constitute an act of cyber war, and as such we could say that nations have been at cyber war in the past and are likely to continue to engage in cyber war in years to come. For this essay, I will use Stones definition to argue that even though states may engage in cyber war, the concept of cyber war is exaggerated. It seems that cyber war is deliberately exaggerated in the media and by politicians for financial and political gains. There are countless examples in the media and in politics of the exaggeration of the threat of cyber war and the language used plays a big factor in creating a sense of fear in the community. The Four Corners report, Hacked, is a classic example where the reporter, Andrew Fowler describes the current situation in Australia as ‘… a secret war where the body count is climbing every day’ (Fowler 2013). The documentary reveals nothing violent or lethal about cyber incidents. The documentary is actually about hackers working from locations overseas, having targeted key Federal Government departments and major corporations in Australia. In another example, NATO may be interpreted as exaggerating the threat of Cyber War when they invited Charlie Millar to present at their Conference for Cyber Conflict at the NATO Cooperative Cyber Defence Centre of Excellence in 2017. Millar is an independent security evaluator, and his presentation was titled ‘Kim Jong-il and me: How to build a cyber army to attack the US’. He later presented similar content at Def Con 2018. His presentation described the steps he would take to mount a cyber war, including the types of people he would engage, how much he would pay them, what his strategy would be and how much it would cost in total. Who stands to gain from the exaggeration and hype? Logically, one group would be those that gain financially from the sale of cyber protective services and software. According to Valerino, 57% of technical experts surveyed said that we are currently in a cyber arms race and 43% said that the worst-case scenarios are inevitable (Valeriano and Ryan 2015). Translate this into sales and Gartner projects worldwide security spending will reach $96 Billion in 2018, up 8 Percent from 2017 and to top $113 billion by 2020 (Gartner 2017). Additionally, there may be political motivations to exaggerate the threat of cyber war. Cyberspace is not well understood by the general public and fear is natural. In the US’s cyber security debate, observers have noted there is a tendency for policymakers, military leaders, and media, among others, to use frightening ‘cyber-doom scenarios’ when making a case for action on cyber security (Dunn 2008, 2). There is some evidence to suggest that more recently in the political arena; we may be maturing in our understanding of the real threat of cyber war. The Tallinn Manual, an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare, was written at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence. It was first published in 2013 with the title ‘The Tallinn Manual on the International Law of Cyber War’. In 2017, it was re-released with the revised title ‘Tallinn Manual 2.0 on the International Law of Cyber Operations’. The change in title from ‘war’ to ‘operations’ signifies a more moderate use of language from NATO and is an acknowledgement that cyber incidents generally fall below the threshold at which International Law would declare them to be a formal act of war. Experience over the 4 short years from 2013 to 2017 has demonstrated that cyber incidents tend to have a low-level impact on the target state. As the book’s authors put it ‘the focus of the original Manual was on the most severe cyber operations, those that violate the prohibition of the use of force in international relations, entitle states to exercise the right of self-defence, and/or occur during armed conflict’ while the new version ‘adds a legal analysis of the more common cyber incidents that states encounter on a day-to-day basis and that fall below the thresholds of the use of force or armed conflict’ (Leetaru 2017). To get a better sense if cyber war is exaggerated, we must also consider the probability of cyber war in the future. The probability of cyber war should be weighed up against the probability of conventional war. Where tensions are already high, for example, between North Korea and the US or Russia and Estonia, I would argue that cyber war is more likely than conventional war. This is due to factors including; cyber warfare is less costly than conventional warfare, states are less rational in their decision space in the cyber realm, states find cyber attribution very difficult to achieve so attacks can be undertaken covertly and cyber war is considered ‘a challenge’ and central to the hackers’ ethos (Junio 2013, 128). Further, Sanger describes in his book, The Perfect Weapon, cyber weapons (such as cyber vandalism, Distributed Denial of Service (DDOS), intrusions and advanced persistent threat (APT)) as the ‘perfect weapons’ for the following reasons; They are cheap: When compared to Nuclear weapons, there are only a handful of nations globally that can afford the technology to create a nuclear weapon. They are easily accessible: Unlike a Nuclear bomb that requires uranium, a highly protected metal, in the production process, a cyber weapon can be created with minimal investment and highly available IT infrastructure. They can be dialled-up or dialled-down relatively easily. A ballistic missile, the force of the explosion cannot be adjusted as easily as a DDOS attack. A DDOS attack can be adjusted to last an hour, a few days or a few weeks. They have a huge range in how they are used: Sabotage as with Stuxnet, Espionage as with the Chinese industrial spying on the US, North Korea’s infiltration of Sony, the Iranians attack on Las Vegas Sands Corp. casino operators. The significant factor is that cyber weapons can and are being used every day for discrete, low-level cyber conflicts to undermine and disrupt rivals, but historically it has not progressed to open conflict, nor has it warranted a military response (Sanger 2018). Additionally, massive cyber operations would necessarily impact the civilian population and violate the immunity of non-combatants. The conditions of war dictate that this is “taboo” and to date, rival states have shown restraint in their use of cyber weapons for this reason (Valeriano and Ryan 2015). It appears that the threat that cyber weapons represent to national security is overstated and the threat of cyber war is overstated. The US and likely other highly networked nations appear reticent about using cyber weapons for significant cyber conflict given their vulnerabilities. Ironically, NSA programs such as PRISM have made the US more of a target given the sheer volume of sensitive information stored in one place. Regardless of US defences, there is no way to make this information completely secure from intrusion, and as such, the very act of storing the information makes them more vulnerable. Rid (2012) is among some academics who argue that cyber war has never and will likely never eventuate. The benefits of being on this side of the debate mean that public funding can be allocated away from offensive cyber security initiatives to other, potentially more important initiatives, such as public health and housing. The government is constantly under pressure to prioritise public spending and it is imperative that they have realistic, accurate projections regarding the risk of cyber war, the probability and the impact, to allow them to focus spending on the most important areas.

### Ext --- Top Level Cyber D

#### No attacks nor impact.

Lewis ’20 [James Andrew; 8/17/20; senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies; "Dismissing Cyber Catastrophe," https://www.csis.org/analysis/dismissing-cyber-catastrophe]

A catastrophic cyberattack was first predicted in the mid-1990s. Since then, predictions of a catastrophe have appeared regularly and have entered the popular consciousness. As a trope, a cyber catastrophe captures our imagination, but as analysis, it remains entirely imaginary and is of dubious value as a basis for policymaking. There has never been a catastrophic cyberattack.

To qualify as a catastrophe, an event must produce damaging mass effect, including casualties and destruction. The fires that swept across California last summer were a catastrophe. Covid-19 has been a catastrophe, especially in countries with inadequate responses. With man-made actions, however, a catastrophe is harder to produce than it may seem, and for cyberattacks a catastrophe requires organizational and technical skills most actors still do not possess. It requires planning, reconnaissance to find vulnerabilities, and then acquiring or building attack tools—things that require resources and experience. To achieve mass effect, either a few central targets (like an electrical grid) need to be hit or multiple targets would have to be hit simultaneously (as is the case with urban water systems), something that is itself an operational challenge.

It is easier to imagine a catastrophe than to produce it. The 2003 East Coast blackout is the archetype for an attack on the U.S. electrical grid. No one died in this blackout, and services were restored in a few days. As electric production is digitized, vulnerability increases, but many electrical companies have made cybersecurity a priority. Similarly, at water treatment plants, the chemicals used to purify water are controlled in ways that make mass releases difficult. In any case, it would take a massive amount of chemicals to poison large rivers or lakes, more than most companies keep on hand, and any release would quickly be diluted.

#### Their evidence is hyperbole.

Valeriano & Maness 18 Brandon Valeriano, PhD, Chair of Armed Politics at the Marine Corps University, Cyber Security Senior Fellow at the Atlantic Council, & Ryan Maness, an American cybersecurity expert, Defense Analysis Professor at Naval Postgraduate School. [How We Stopped Worrying about Cyber Doom and Started Collecting Data, Politics and Governance, 6(2), Cogitatio Press]

Moderate and measured takes on cyber security threats are swamped by the recent flood of research and policy positions in the cyber research field offering hyperbolic perspectives based on limited observations. This skewed perspective suggests constant cyber disasters that are confronting humanity constantly. The general tone of the debate argues that cyber war is already upon us and our future will only witness more cyber doom. However, these hyperbolic perspectives are being countered by empirical investigations that produce the opposite of what is to be expected. It is generally observed that limited cyber engagements throughout the geopolitical system are the dominant form of interaction. Our task here is to offer a different path forward. We first posit what can be known about cyber security interactions with data as well as what cannot. Where is the water's edge in cyber security research? We then examine the known works in the field that utilize data and evidence to examine cyber security processes. Finally, we conclude with an offering of what types of studies need to be done in the future to move the field forward, away from the prognostication and generalizations so typical in the discourse in this constantly changing and growing field. Keywords cyber conflict; cyber security; cyber strategy; data collection; quantitative methods Full Text: 1. The Challenge of Cyber Security Threat Data Beginning in 2014, various news organizations began reporting on a particular cyber security firm, Norse Corporation, and their active cyber threat map (Walker, 2015). Mashable noted in 2016 that "the global cyber war is raging on, and this mesmerizing map shows just how serious it has become" (Gallucci, 2016). The map is dynamic, colorful, and gets the point across quickly, a criterion for any decent visualization of data. As late of August 2017, the Defense Intelligence Agency (DIA) tweeted out a link and photo of the threat maps suggesting it represented ongoing cyber-attacks (DIA, 2017). Yet this map is not a very clear representation of any real threats that nationstates face on a daily basis. Unfortunately, the Norse cyber threat map does not represent active threat data, but attacks, likely by bots, on preset honeypots. Honeypots are a method of providing data on fake targets to either distract the opposition from the real targets or to deter an aggressor from attacking in the first place (Gartzke & Lindsay, 2015). While sometimes a useful method to gather threat intelligence if presented a sleight of hand for an attractive target, honeypots as reported in popular discourse are not exactly an accurate representation of the cyber threat landscape. In this case, the goal was to demonstrate the ability to track global attacks to gain interest in the company and promote its capabilities. Nearly all active threat maps either present data tracking honeypots and various bot networks that are devoid of human agency, simply presenting what is in fact fake data. Active representation of the threat landscape is the goal, but the reality is that the picture of the cyber security threat landscape we currently have is incomplete, misleading, or outright fake. High profile data breaches have been consuming media narratives for at least a decade. With each act of cyber disruption or espionage, pundits as well as government officials and several academics declare that cyberwar-fare is upon us, is the future of warfare, and it is only a matter of time before a "Cyber Pearl Harbor" wreaks havoc on the American homeland (Gurdus, 2016). With this new revolution in military affairs, the battlefield, according to some, is forever changed and the next big war could very well be a cyberwar (Clarke & Knake, 2010; Kello, 2013). Politicians, pundits, and practitioners have jumped on this doomsday narrative and have promoted cyber arms races, offensive advantage, and deterrence strategies to stay one step ahead of would be adversaries in order to prevent them from infiltrating networks out of fear of massive retaliation. These revolutionists point to acts such as Stuxnet, Shamoon, Sony, and the Office of Personal Management (OPM) hack as the new norm of conflict between states, and that the US is losing ground with every tolerated cyber-attack on American networks.

### 1NC --- Cyber Grid D

#### No grid hacks---AND squirrels thump.

Larson 19, Intel Analyst @ Dragos. (Selena, 4-3-2019, "Debunking the Hacker Hype: The Reality of Widespread Blackouts", *Dragos*, <https://www.dragos.com/blog/industry-news/debunking-the-hacker-hype-the-reality-of-widespread-blackouts-rsa-2019-recap/>)

Unfortunately, the Hollywood-esque idea of a country-wide blackout that grinds society to a halt is what many people consider to be the reality of the threat to the electric grid system. But the truth is less of a blockbuster.

Consider this:

A destructive incident at one site would require highly-tailored tools and operations and would not effectively scale.

A ransomware infection at the financial services division of an electric utility doesn’t automatically translate into a blackout.

In most industrial environments the equipment can operate safely and independently for quite a while, so system downtime may have no effect. It could however hurt business operations like shipping, sales, etc.

So why is it important to identify fear, uncertainty, and doubt (FUD) in reporting? It can have a real impact on how people do their jobs: if incidents relating to ICS security are misreported it can be a headache for defenders and owners and operators who may not have the proper context. Additionally, it contributes to an overall misunderstanding among the general public and policy makers who often make decisions based on public information.

It’s worth noting the phrase “hacking the grid” doesn’t make complete sense. At a very basic level, the North American Electric grid is complex and made up of regional and local electricity grids that are connected together to make larger networks for reliability. There are also built-in redundancies for power resiliency. Cyberattacks are not the only threats grid operators and other stakeholders consider when focusing on defending the US electric grid. The long-running joke is that squirrels and other animals should be considered their own APT group due to their ability to cause blackouts; it is, however, true that creatures, natural events, vegetation like fallen limbs, and physical disruptions are all potential threats to grid systems.

### Ext --- Cyber Grid D

**New grid tech solves resilience vs cyber**

**TULLY 21** --- SHAWN TULLY , “A new technology being used in Chicago could protect cities from blackouts and cyberattacks”, Fortune, Aug 31st 2021, https://fortune.com/2021/08/31/chicago-reg-resilient-electric-grid-system-preventing-blackouts-cyberattacks/

A new partnership between a pioneer in superconductor technology and the Chicago utility has hatched a new solution for keeping the heat pumping and factories chugging if anything were to knock out parts of the city’s grid. American Superconductor (AMSC), a Nasdaq-listed innovator in energy technology, is deploying its Resilient Electric Grid (REG) system at two substations operated by ComEd, the utility serving over 4 million homes and businesses in Chicago and northern Illinois. If this first installation performs as the city expects, Chicago could expand the technology to link many more of the nodes that distribute electricity directly to homes and businesses. “We’re planning this stage with the next stage of connecting multiple substations in mind,” says Terence Donnelly, president and COO of ComEd. Put simply, REG is a backup system that for the first time connects substations so that if a downtown facility is damaged by severe weather or a massive hack, a nearby station it’s linked to sends power to the offices and apartment buildings that would otherwise suffer a blackout.

The REG technology offers a second big advantage. It could create a fully integrated network where when one substation needs extra power, others that harbor additional capacity can fill the gap. Hence, utilities would no longer need to build each individual station so that it holds tons of excess capacity for times when AC units or heaters are running at full tilt, or when part of its equipment fails. “**REG changes the whole geography of the grid,”** says Daniel McGahn, AMSC’s chief executive. “The more you network the grid**, the less excess capacity you need.** The utilities no longer have to keep building new substations to meet higher usage, they can tap the ‘trapped’ capacity from the substations already there.”

The way the grid operates now, its nodes can’t back each other up in times of trouble

To grasp the potential impact of the REG system, it’s important to understand why the design of today’s grids prevents them from sharing electricity. The grid resembles the hub and spokes of a bicycle wheel. Huge power plants that run on natural gas, nuclear, wind, and solar—mostly located far from the cities they serve—send electricity via “long-haul” transmission lines to substations in urban neighborhoods. ComEd has several hundred substations in the city of Chicago alone. Some get their power from a single plant, others from a blend of, say, renewables and natural gas from multiple facilities.

The substations are equipped with transformers that collect all that high-voltage electricity, and step down the voltages to a level that’s safe for homes and stores. The stations’ circuit breakers cut off the power flowing from the big plants if too much voltage is arriving. By the way, you seldom see or recognize a substation while walking around a city. They’re often installed in a brownstone that just looks like a residence, or sheltered in the basements of apartment buildings. That’s a sketch of the transmission and distribution system as it stands today.

The spokes are the lines that run directly from the substations to the homes, apartment buildings, and businesses in their service areas. But the hubs or nodes in the system, the substations, aren’t connected to each other. Their function is strictly distribution, sending the electricity from power plants to their customers. They don’t form a network at all. They can’t back each other up by having substation A that has excess capacity channel electricity to substation B when B is short on power or has shut down during a heat wave, a cyber hack, or an equipment failure.

Because today’s substations operate as islands or silos, each one needs to be designed with far more capacity than it uses most of the time. The reason is twofold. First, the stations must contain transformers and other gear big enough to meet times of peak demand, such as 100-degree days when everyone’s running the AC to keep cool. Second, some of the equipment at a substation will occasionally malfunction. So they need even more backup so that the gear that remains working can compensate for the parts most likely to break down. “All told, most substations have built-in redundancy of 100%,” says McGahn, meaning they’re designed and constructed to generate twice as much juice as their customers consume on a typical day.

Obviously, connecting substations would be a **great solution**. Today, in case of a cyberattack on one substation, the other stations loaded with excess capacity can’t send their power to light and heat the homes suffering the blackout. Nor can a substation in the suburbs that has extra capacity on a hot day dispatch it to a maxed-out station in a city center.

But the stations couldn’t link up for two reasons. First, the traditional copper cables used to move power were too bulky to fit into the rights-of-way for the much smaller conduits running from the stations to homes and buildings. Second, if and when a substation sends power to another substation, that power starts in a big surge. That surge is powerful enough to knock out the transformers in the station receiving the electricity. Worse, if several substations are connected, the rush can cause a domino effect that disables a whole series of stations. The supposed solution would turn into a disaster on the scale of a cyber hack. That cascading effect is how many blackouts in the past have occurred.

**How the new REG technology would harden and expand the grid**

AMSC’s superconductor technology miniaturizes power transmission. Its Amperium wire is made from a copper oxide compound that, for the same weight, enables it to carry 200 times the voltage of the regular copper wire that’s the traditional foundation for transmission. When electricity travels one mile over copper cable, as much as one-third of the power is lost during that trip. By contrast, electricity can cover any distance over superconductor wire and suffer no electrical loss.

The U.S. Navy deploys the AMSC's Amperium superconductors to protect its ships from mines. The technology is calibrated to mask the magnetic field spread by the vessels so they don’t trigger the underwater explosives. But utilities were still reluctant to deploy superconductors for joining substations. They acknowledged that superconductors solved the space problem: They can fit inside six-inch–diameter conduits and pipes that run well within the rights-of-way going from the substations to customers. The rights-of-way for each substation overlap with those of other stations, making it possible to extend the wires from one substation to another in the next neighborhood, or even 50 miles away.

The obstacle: The superconductor technology hadn’t solved the “overcurrent” problem that could cause rolling blackouts. But AMSC’s Amperium was the breakthrough. It combined the ability to carry huge amounts of power over a small wire with an outer layer called a “super-resistor” that tames the surges, and also protects against lightning strikes that could cause cascading outages.

What the Chicago project could mean for cybersecurity and more

As McGahn puts it, the REG technology provides an extension cord between the now-vulnerable nodes in the nation’s urban power grids. If substations are linked, power from those still functioning **would automatically flow to the customers of the station that’s attacked** or hit by extreme weather. In addition, utilities will be getting far more of their power from renewable sources in the future, and that power shuts off when the wind’s not blowing or even when the sun goes behind a cloud. Grids will need a lot more backup capacity to compensate for that intermittent energy. Linking substations would provide that support without needing to continue the current strategy of building still more substations to ensure sufficient backup.

The Chicago project links just two substations. For McGahn and ComEd the ideal solution is joining many or even all the nodes in one giant network that operates in a kind of buddy system. McGahn wants to create a “super-grid” that allows for more renewables without adding lots of backup capacity, and hence at a much lower cost than would be required under the current system. His vision would make our grids much safer, and enable the grid to channel electricity where it’s needed, when it’s needed, in exactly the amounts it’s needed, with far less need for excess capacity.

It’s a big vision for an old, and some would say stodgy, industry. But it would unite aging infrastructure with new technology to make America’s most vulnerable pressure points, where terrorists and hackers are now taking aim, **far more secure.**

#### Critical infrastructure can easily manage risks.

Pfeiffer et al. 17, Kyle B. Pfeiffer, Director of the National Preparedness Analytics Center within the Decision and Infrastructure Sciences Division at Argonne National Laboratory, M.S. in Science and Technology Leadership from Brown University; Carmella Burdi, Senior Geographic Information Systems Analyst in the Decision and Infrastructure Sciences Division at Argonne National Laboratory, M.S. in Geographic Information Systems from Northwest Missouri State University; Scott Schlueter, Senior Geographic Information Systems Analyst at Argonne National Laboratory, M.S. in Geographic Information Science and Cartography from the University of Washington, “Local Supply Chains: the Disaster Management Perspective,” International Journal of Safety and Security Engineering, Vol. 7, No. 3, 2017, https://www.witpress.com/elibrary/sse-volumes/7/3/1886

Managing risk, even for a simplistic supply chain, has become a professional responsibility. In the United States, both small and large private sector organizations employ logisticians, continuity experts, and risk analysts to help identify and mitigate risks to their enterprise. Their focus can be everything from coordination of supply and demand to minimizing disruption of normal activities. For the purpose of this research, disruption risks are examined, as they are more likely to intersect with the roles and responsibilities of public safety officials. [2] Furthermore, those in the public sector may be able to effect the most change around them. Disruption risks can be described in four broad categories: operational contingencies, natural hazards, terrorism, and political instability. Operational contingencies are systematic failures, such as the August 2003 Northeastern United States grid blackout, which caused curtailment of operations for many supply and demand nodes. [2, 3]. Natural hazards are events such as hurricanes, wildfires, earthquakes, or flooding which can disrupt critical components of a supply chain – such as the fuel shortages in the New York–New Jersey area following Superstorm Sandy in 2012. [4] Terrorism, the next category of disruption risks, may include indiscriminate destruction of critical supply chain components or targeted sabotage of known critical assets and systems. [3] Lastly, political instability may disrupt supply chains, such as oil production curtailment in Iraq and Syria, given the regional strife since 2012.

In the United States, operational contingencies and natural hazards are among the most likely disruption risks to significantly affect supply chains that are critical to communities following a disaster. The effects of these disruptions may directly impact the ability of a community to obtain food, fuel, prescription medication, or other critical goods and services in the minutes, days, or weeks following a disaster. Understanding the behavior of these supply chains, particularly in near real-time after a disaster, may help officials to make more informed decisions regarding response and recovery activities.

#### Cyber attacks won’t take down the grid

Victoria Craig 16, Analyst at Fox Business, Citing the Senior Manager of Industrial Control Systems at Mandiant, “The U.S. Power Grid is 'Vulnerable,' But Don't Panic Just Yet”, http://www.foxbusiness.com/features/2016/02/02/u-s-power-grid-is-vulnerable-but-dont-panic-just-yet.html

The idea of the nation's power grids becoming the next battleground for cyber warriors could make hacking into consumers’ credit card accounts and personal information seem like child’s play. While U.S. power companies are likely targeted by foreign governments and others in increasingly sophisticated breaches, actually shutting off the lights and causing chaos is far more complicated than many pundits make it seem. Dan Scali, senior manager of industrial control systems at Mandiant, a cybersecurity consulting arm of FireEye ([FEYE](http://www.foxbusiness.com/quote.html?stockTicker=FEYE)), explained that while cyber criminals may gain access to power and utility data systems, it doesn’t necessarily mean the result will be a power outage and a total takedown of power grid control systems. In other words, the power grid is controlled by more than just a panel of digital buttons. “Losing the control system is bad from the perspective that it takes you out of your normal mode of operations of being able to control everything from one command center, but it doesn’t mean you’ve lost control or all the lights go out [in the city],” Scali explained. While many of the systems have been modernized to include digitized control panels, if a hacker were to infiltrate the system, a utility worker could still have the ability to manually control the machines by flipping a switch, pushing a button, or tripping a breaker. As the world saw with the recent attack in Ukraine, which caused a blackout for 80,000 customers of the nation’s western utility, the biggest problem may be ensuring the power grid’s control systems are not vulnerable to cyber break ins. The January attack in Ukraine was likely caused by a corrupted Microsoft Word attachment that allowed remote control over the computer, according to the U.S. Department of Homeland Security. Scali said there was no evidence from the incident in Ukraine that the hacker’s malware was able to physically shut down the power. “It wiped out machines, deleted all the files. Kill disk malware made it impossible to remotely control things. It caused chaos on the business network, and the area where control system operations sat. But the attacker, we believe, would have had to actually used the control system to cause load shedding, which caused the power to go out, or trip breakers to cause the actual problem. Malware itself didn’t turn the power out,” Scali said. He said what most likely happened in that incident was the hacker stole user credentials and logged into the system remotely. The bottom line: Yes, a similar event could happen in the U.S. And corporate America is concerned. A recent survey released in January on the state of information security, conducted by consulting firm Pricewaterhouse Coopers, showed cybersecurity as one of the biggest concerns among the top brass at U.S. power and utilities firms. Part of the problem, Brad Bauch, security and cyber sector leader at PwC said, is the interconnectedness of the industry’s tools. “Utilities want to be able to get information out of [their] systems to more efficiently operate them, and also share that information with customers so they have more real-time information into their usage,” he explained. While allowing access to their own consumption data allows the companies to give their customers more of what they want, it also opens up a host of access points for hackers, making the systems more vulnerable than they otherwise would be. But to say that the power grid is susceptible to cyber hackers is a bit of an oversimplification.

#### Grid’s resilient---no collapse

Jim Avila 12, Senior National Correspondent at ABC News, “A U.S. Blackout as Large as India’s? ‘Very Unlikely’”, http://abcnews.go.com/blogs/headlines/2012/07/a-u-s-blackout-as-large-as-indias-very-unlikely/

As India recovers from a blackout that left the world’s second-largest country — and more than 600 million residents — in the dark, a ripple of uncertainty moved through the Federal Regulatory Commission’s command center today in the U.S. The Indian crisis had some people asking about the vulnerability of America’s grid.

“What people really want to know today is, can something like India happen here? So if there is an outage or some problem in the Northeast, can it actually spread all the way to California,” John Wellinghoff, the commission’s chairman, told ABC News. “It’s very, very unlikely that ultimately would happen.”

Wellinghoff said that first, the grid was divided in the middle of the nation. Engineers said that it also was monitored more closely than ever. The grid is checked for line surges 30 times a second.

Since the Northeast blackout in 2003 — the largest in the U.S., which affected 55 million — 16,000 miles of new transmission lines have been added to the grid.

And even though some lines in the Northeast are more than 70 years old, Wellinghoff said that the chances of a blackout like India’s were very low.

### 1NC --- Cyber Shipping D

#### No impact---technically impossible and the explosion is contained.

Chalk 10—Adjunct Political Scientists at RAND, Adjunct Professor at the Naval Postgraduate School in Monterey, and a PhD in political science from the University of British Columbia [Peter, “Assessing the Recent Terrorist Threat to the Malacca Strait,” *CTC Sentinel*, Vol. 3, Iss. 4, April, p. 9-11, Emory Libraries]

While there is little doubt concerning the economic salience of the Malacca Strait, carrying out decisive attacks against ships transiting through this corridor is somewhat more challenging than commonly portrayed. One of the most frequently postulated scenarios is that terrorists could attempt to disrupt the commercial viability of the Strait, either by detonating a hijacked oil or LNG tanker to shut down a prominent commercial terminal (such as the Port of Singapore) or by scuttling a large ship to block the through-passage of maritime traffic.8 Although theoretically possible, realization of both attack contingencies would be difficult to achieve.

Igniting pressurized LNG or oil is technically problematic. Unless these substances vent in their liquid form and mix with air in the correct ratio, the probability of either substance fully catching fire is extremely low. Even if this did occur, the lateral force of any subsequent explosion would likely be contained by the tanker’s hull, which would force the destructive energy upwards rather than outwards (thus minimizing its destructive potential).9 Sinking a major oceangoing freighter is equally as challenging and would, at a minimum, require the perpetrating group to have ready access to a large quantity of explosives, the time and means to transport this material and the expertise to know where to place the bombs to cause a critical breach. These logistical and knowledge barriers would pose formidable barriers for a single attack—much less an assault that targeted two or three ships (which would be required to truly block the Strait).10

### Ext --- Cyber Shipping D

#### Attacks will be limited --- can’t escalate

Valeriano & Maness 18 – Brandon Valeriano, PhD, Chair of Armed Politics at the Marine Corps University, Cyber Security Senior Fellow at the Atlantic Council. Ryan Maness, an American cybersecurity expert, Defense Analysis Professor at Naval Postgraduate School. [How We Stopped Worrying about Cyber Doom and Started Collecting Data, Politics and Governance, 6(2), Cogitatio Press]

6. Expanding Cyber Security Data Our team has been coding cyber incident data since 2010 and serves as a unique example of how the process of collecting cyber security data and evidence can be done. Our first peer reviewed published work appeared in 2014 in Journal of Peace Research (Valeriano & Maness, 2014). In this article we note that cyber conflict is much more restrained than generally understood by popular discourse. Threat inflation is ripe in cyber security, and the real use of cyber tools seems to be to enhance the power of strong states.

The data that Valeriano and Maness (2014, 2015) have built challenges the cyber revolution perspective and does so with the tools of social science, and is a necessary turn given the general tone of the debate. We first determine that a viable data collection method in light of limited resources was to focus on states that are committed interstate rivals (Diehl & Goertz, 2001). This allows us to focus on those actors with an intense history of recent hostilities that should be the most likely users of cyber technology on the battlefield (Maness & Valeriano, 2018).

In our research (Maness & Valeriano, 2016; Maness, Valeriano, & Jensen, 2017; Valeriano & Maness, 2014, 2015), we have been able to marshal a massive amount of evidence that is useful in dissecting the actual trends on the cyber battlefield in a geopolitical context. We demonstrate that while cyber-attacks are increasing in frequency, they are limited in severity, are directly connected to traditional territorial disagreements, and mostly take the shape of espionage and low-level disruptive campaigns rather than outright warfare.

Given this data-based perspective, we question the dynamics of the cyber security debate and offer a countering theory where states are restrained from using more malicious cyber actions due to the limited nature of the weapons, the possibly of blowback, the connection between the digital world and civilian infrastructure, and the reality that any cyber weapon launched can be replicated and used right back against the attacker. Given all of these perspectives gleamed from the data, we must moderate our views about the transformation that is offered by cyber strategists who stress a more revolutionist tone (Lango, 2016).

Social science clearly matters for contemporary technological policy debates. Absent rigorous methods, much of what is in the field is basically guesswork. Our work really owes an intellectual debt to J. David Singer, who started the effort to quantify war at the University of Michigan with the Correlates of War (COW) project (Small & Singer, 1982). Our project builds on this methodology and uses many of the same coding strategies. We recognize that data is a work in progress and seek to build more and more knowledge through subsequent updates. By gathering the full picture, we can gain the perspective that really matters in these emerging policy debates regarding the cyber battlefield.

#### Err against catastrophe.

Lewis ’20 [James Andrew; 8/17/20; senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies; "Dismissing Cyber Catastrophe," https://www.csis.org/analysis/dismissing-cyber-catastrophe]

This is a short overview of why catastrophe is unlikely. Several longer CSIS reports go into the reasons in some detail. Past performance may not necessarily predict the future, but after 25 years without a single catastrophic cyberattack, we should invoke the concept cautiously, if at all. Why then, it is raised so often?

Some of the explanation for the emphasis on cyber catastrophe is hortatory. When the author of one of the first reports (in the 1990s) to sound the alarm over cyber catastrophe was asked later why he had warned of a cyber Pearl Harbor when it was clear this was not going to happen, his reply was that he hoped to scare people into action. "Catastrophe is nigh; we must act" was possibly a reasonable strategy 22 years ago, but no longer.

The resilience of historical events to remain culturally significant must be taken into account for an objective assessment of cyber warfare, and this will require the United States to discard some hypothetical scenarios. The long experience of living under the shadow of nuclear annihilation still shapes American thinking and conditions the United States to expect extreme outcomes. American thinking is also shaped by the experience of 9/11, a wrenching attack that caught the United States by surprise. Fears of another 9/11 reinforce the memory of nuclear war in driving the catastrophe trope, but when applied to cyberattack, these scenarios do not track with operational requirements or the nature of opponent strategy and planning. The contours of cyber warfare are emerging, but they are not always what we discuss. Better policy will require greater objectivity.

### Ext --- Shipping Not K2 Trade

#### Trade resilient despite shipping cost

Fechner 22 --- Inga Fechner, economist at ING in Germany, covering international economic developments with a specific focus on Austria, and Rico Luman is a senior sector economist with a focus on transport, logistics and the automotive industry, “Trade Outlook 2022: Clogged supply chains won’t hold trade back”, ING, 26 January 2022, https://think.ing.com/articles/trade-outlook-2022-clogged-supply-chains-wont-hold-back-trade

Despite the profound disruptive impact of the pandemic on supply chains, demand for consumer goods rose strongly last year. We expect merchandise world trade volumes to have increased by 10.6% in 2021 compared to the previous year, surpassing its pre-pandemic level by 4.3%. The growth rates of global merchandise trade should return to pre-pandemic levels this year, supported by industrial growth, global demand for goods remaining elevated, and only a limited shift of consumption back to services.

And that double-digit expected increase comes in spite of massive supply chain disruptions and soaring transport costs. It reflects strong demand for goods during the pandemic with China being one of the main drivers of the trade surge.

When we look at the details, world trade volume increased 2% month-on-month in November 2021, the second increase in a row. That's according to the World Trade Monitor for November from CPB. An increase in exports (+2.8%) and imports (+3.6%) mainly in advanced economies led to the rise in trade volumes, while China's exports decreased 4.1%. Imports showed modest growth of 1.2%. With some delay, this is also reflected in global container throughput which is regaining traction.

World trade normalises and continues to grow despite challenges

Going into 2022, we expect trade growth rates to return to their pre-pandemic levels in line with a continued but weakened global economic recovery. For this year, we pencil in a growth rate in merchandise world trade of 4.1% compared to 10.6% the year before, while we expect world GDP growth to come in at 4.4% from 6.1% in 2021. 2021 was an exceptional year driven by pandemic-related catch-up effects. Despite ongoing supply chain frictions and average containerised transport costs expected to remain high, we still expect to see a decent growth rate.

We expect the global economy will gain traction and enter a new phase should the Omicron wave become significantly less of a threat by the European spring. The experience of almost two years of crisis shows that economies can adapt, suggesting any new regional lockdowns should have less of an impact. That said, a shift by consumers back into services will only be moderate in 2022 because of Covid caution. They might reduce some of their increased spending on the likes of electronics and furniture while resuming spending on services all the while seeing higher energy and food prices. Overall, however, the preference for goods remains elevated.

In the US, for example, the share of goods spending as a proportion of total personal consumption expenditure continues to hover around 35%, well above its 31% average in 2019. This indicates a continued goods' preference in the first quarter of 2022.

Ongoing labour shortages around the globe argue in favour of a rebound in wage growth and an improvement in workers’ bargaining power. This, in turn, means we should see an environment of continued elevated demand, fueling world trade volumes. However, there is a risk that real wages will remain negative despite those higher wages with worldwide inflation expected to surge to 4.6% this year.

Through 2022, however, we expect inflation to subside, which leaves room for real income growth to turn positive in the second half of the year. In the eurozone, data seems to confirm this with manufacturers mentioning easing sourcing constraints which in part helped to ease input price inflation to the lowest level since last April. Governmental fiscal support and infrastructure plans, partly related to the green transition, also point to a continued positive investment outlook despite a tightening of financing conditions from major central banks,

Asia to remain a driving force in 2022

Trade growth remains uneven, however, when you look at different regions. The divergence across blocks and individual countries has been - and will be - driven by the progress and speed of vaccinations and the dependence on intermediate goods. Intra-Asia trade still has strong growth perspectives. Following an improvement in Asian industrial production over 2021 as well as significantly higher container throughput in Shanghai (+8%) and other major Chinese ports, the general macroeconomic outlook for Asia and especially China depends on Covid, chip shortages and the US relationship.

A slowing of economic activity in China remains a concern for northeastern Asian industrial economies. Cooling industrial demand for coal and iron ore from China has already led to bulk freight rates easing after a commodity-driven peak. Chinese trade flows may also be more volatile this year due to less real estate construction but more infrastructure investment may help to balance that out.

On a global level, we expect larger flows of oil and oil products alongside the global recovery of road and airline traffic and we think that China should remain a major driver of growth for metals exposed to the energy transition. We expect global automotive production to increase by up to 10% (we've written more about that here) and that will create extra trade volumes but the semiconductor shortage will be a limiting factor.

Lastly, the implementation of regional trade agreements such as the Regional Comprehensive Economic Partnership (RCEP) within the Asia-Pacific area coming into force as of the beginning of the year or the African Continental Free Trade Area (AfCFTA) promoting intra-African trade, will likely affect regional trade flows.

Supply chain slump and elevated tariffs will drag through 2022

So it all looks positive but it doesn't mean we don't face any obstacles to our growth outlook. A combination of shipping capacity and container shortages, unforeseen incidents, whether those be terminal closures in China or another blockage of the Suez Canal, and we could also see labour shortfalls which helped lead to spiking container rates last year. And 2022 started off with new records here. Based on UNCTAD data, those costs pushed China to Europe port-to-port container costs up to some 15% of the average goods transported (up from 2-3%).

The effect of massive port congestion occupying 10-15% of the global fleet capacity feeds back to that disruption. We've perhaps seen the biggest impact of that in the US. Container ships waiting at Los Angeles-Long Beach (covering 40% of US containerised imports) hit record levels in January with shortages at port sites and a lack of truck drivers to push goods further down the line. In Europe, the effect is less pronounced but still, ports are packed too. In China, we have seen similar squeezes in the Ningbo, Tianjin and Zhenzhen ports because of the country's zero-Covid policy. After Chinese New Year we do expect things to improve. But when spot rates come down, term contract rates of large shippers are still being negotiated higher.

We concluded earlier that container rates will remain under upward pressure and won’t return to pre-pandemic levels anytime soon. A record wave of newly ordered ultra-large container vessels will come online from 2023 and 2024 but the container shipping sector is much more consolidated with three large alliances. Container liners also have learned to manage capacity better. The container sector is also entering the energy transition with retailers aiming to reach zero-emission seabound trade by 2040 and companies are facing some sort of CO2 pricing. Maersk already started the shift by ordering 12 methanol-ready container vessels. But, in any case, fuel is expected to be more expensive, and that has an upward pressure on prices too, of course.

Risks ahead but trade fundamentals are still solid

The pandemic remains an uncertain factor affecting the outlook for 2022. Supply chain troubles and higher shipping costs also continue to pose risks to growth. At the same time, last year also showed this doesn’t necessarily hamper the world from continuing to trade.

The economics of trade still make sense. There are not many examples of re-shoring yet as this takes time; it requires a high level of automation, and it's easier said than done. But shippers do consider multi-sourcing options, buffer stocks and longer contracts and this is still highly supportive.

So, we're optimistic given the economic outlook, a hopefully receding pandemic, and clear evidence of richly filled order books, notably in the automotive sector. We expect trade volume growth to hold up well this year, resulting in a more moderate but still sound growth rate for merchandise world trade.

### Ext --- Trade impact D

#### Trade resilient

Lawrence 21 --- Robert Z. Lawrence, Albert L. Williams Professor of International Trade and Investment, Harvard, “The Unappreciated Trend Toward Unilateral Trade Liberalization”, Peterson Institute For International Economics, March 2021, https://www.piie.com/sites/default/files/documents/pb21-6.pdf

During the 2008 financial crisis, the volume of world trade initially plummeted by more than it had during the Great Depression in the 1930s (Eichengreen and O’Rourke 2010). Since many developing countries could legally raise their applied tariffs without violating their WTO commitments, there were widespread fears that the protectionist responses that had occurred during the Great Depression were likely to be repeated. Yet the system displayed remarkable resilience. Undoubtedly the disastrous experience of the 1930s served as an important consideration motivating the G20 countries to issue statements pledging their opposition to protectionism.12 But their actions spoke even louder than their words.

As shown in figure 1, the crisis is simply not evident in the average global tariff data for 2008 and 2009: The average applied MFN tariff rates in the immediate aftermath of the crisis were no higher than they were before it. This is not to say that no countries raised their tariffs, but the increases were offset by other countries’ reductions.13 In addition, as chronicled by the Global Trade Alert (a network of trade analysts that monitor trade policy actions), some countries did use temporary tariff measures such as safeguards antidumping and countervailing duties.

But studies that take such actions into account still conclude that there was remarkable restraint with respect to import barriers. For example, using an overall Trade Restrictiveness Index that includes not only MFN tariffs but those applied in free trade agreements and other preferential arrangements, Hiao Looi Kee, Cristina Neagu, and Alessandro Nicita (2013) found that together the impacts of tariffs and antidumping measures accounted for less than 2 percent of the collapse of world trade in response to the crisis. Among their explanations is that “countries are likely to take account of the diverse impact of tariffs in raising input costs for products used in their exports” (p. 343).

Looking back from the vantage point of 2019, the Global Trade Alert found that in response to the crisis, “transparent import restrictions were placed on just 1.4 percent of world trade, with another 6.9 and 20.8 percent of world trade being subject to subsidies to import competing firms and state largess to exporters respectively.” However, almost all the temporary import restrictions and half of the subsidies to import-competing firms were unwound by 2013.

Simon Evenett and Richard Baldwin (2020) note that patterns of trade have remained more heavily distorted by export subsidies since the financial crisis; but while they do distort trade, in principle export subsidies should increase rather than reduce trade.

While the declining growth in trade volumes relative to GDP since 2011 has been the focus of much discussion, increased trade protection does not appear to be the reason. As shown in figure 1 there was a small increase in average global tariffs in 2009–11, but it was more than fully reversed by 2012, and by 2017 global trade-weighted average applied MFN rates were considerably lower than they had been in 2008.

Marc Auboin and Floriana Borino (2017) studied the falling elasticity of global trade to economic activity and found that while the slowdown in the growth of global value chains and changes in the composition of demand were important parts of the explanation for slower trade responses to growth after 2011, “protectionism does not come up as statistically significant.”

CONCLUDING COMMENTS

This Policy Brief has provided evidence that even setting aside participation in regional and multilateral trade agreements, developing countries have steadily narrowed the differences between their tariffs and those of the United States. They have also revealed a preference for lower tariffs by consistently applying tariffs that are much lower than those obligated by the WTO. Their commitment to lower tariffs was shown by their discipline in not, on average, raising tariffs in response to the financial crisis in 2008 and their continued reductions in applied tariffs between 2011 and 2017. The available data at the country level show additional reductions in 2018. The commitment to these lower rates is also evident in the regimes for administered protection instituted by several countries, requiring proof of serious injury and other conditions before safeguard protection is provided.

All this liberalizing behavior reflects widespread changes in views of trade protection. The spread of global value chains, which have increased the import content of both exports and domestic production, have convinced many that increased protection can reduce domestic output and employment.

In many industries supply chains consist of production facilities that produce highly customized goods and services that are not easy for firms to produce in other countries or to shift back to their home country. It is noteworthy that, for all their talk about the North American Free Trade Agreement (NAFTA) being a disastrous trade agreement, both President Trump and many Democrats agreed to a US-Mexico-Canada Agreement (USMCA) that made far fewer modifications to the original agreement than might have been expected from their rhetoric.14

Since 2018, however, global supply chains have been subjected to two major shocks: the first from US trade policies and the countermeasures other countries have taken in response, and the second from the COVID-19 pandemic, which initially set off a global scramble for medical equipment. Some commentators have responded to these disruptions by arguing that countries should now be more self-sufficient (Rapoza 2020).15 And it is common to see predictions that the world has now passed the high point of globalization. But it is too soon to tell whether these developments will lead to a reversal of the policy trends discussed in this Policy Brief.

The recent shocks certainly point to the desirability of diversification of supply chains and the need for adequate domestic strategic reserves of essential products. Pinelopi Goldberg (2020) makes the case that they have also underscored the extent to which countries are interdependent. And they have shown the ability of an open global system to enable more resilient responses than those based on self-reliance—the WTO has documented that, in response to the pandemic, trade-facilitating measures undertaken by the G20 have far outweighed trade-restricting measures.16

Indeed, despite the talk of deglobalization, many countries have recently increased their commitments to further trade liberalization, albeit at the regional level. Since 2018, for example, 11 Asia-Pacific countries have implemented the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, more than 50 countries agreed to the African Continental Free Trade Area, and 15 countries in the Asia-Pacific concluded the Regional Comprehensive Economic Partnership in late 2020.

As Mark Twain said about his death, reports of the end of globalization may be greatly exaggerated.

#### No trade impact.

Victoria Pistikou et al. 21, Assistant Professor, International Political Economy, Democritus University of Thrace; Eftychia Tsanana, Lecturer, Economics, University of Macedonia; Thomas Poufinas, Faculty Member, Economics, Democritus University of Thrace, "A Financial Analysis Approach on The Impact of Economic Interdependence on Interstate Conflicts," Theoretical Economics Letters, Vol. 11, No. 5, 09/03/2021, Sci-Hub.

This indicates that the increase of economic interdependence does not lead to a decrease of the interstate conflict as captured by defense expenses. On the contrary the increase of exports of country 1 to country 2 leads to an increase of the expenses of both countries. Hence, both countries seem to consider the conflict as vivid even though some trade activity is built. This may be attributed to the fact that the defense expenses of these countries are not necessarily related to the particular interstate conflict with the investigated pair in the dyad. It could also be due to the fact that the economic crisis has potentially led to a decrease of both the economic activity and the defense expenses in some cases. This explains partially the results. Furthermore, country 1 is not always the stronger economy. In addition, it is not necessarily the country that has initiated the conflict. These findings indicate that the topic needs to be further investigated so as to incorporate more dyads and potentially additional proxies of interstate conflict and economic interdependence in order to realize whether the latter impacts the former.

[Table omitted]

The impact of the independent variables and their explanation is summarized in Table 4.

In political terms, policymakers may find these empirical results interesting as they show that they cannot rely solely on the strengthening of bilateral trade in order to end or reduce the conflict. In addition, according to other studies, establishing a free trade area may be the way for fostering economic ties and interdependence with potential rivals, however, it will be difficult to have a critical impact on conflict if this cannot happen in bilateral level without any degree of economic integration. Therefore, we cannot expect, at least for the mentioned cases, de-escalation or elimination of the conflict caused by increased economic activity between the rivals. Therefore, other routes need to be explored so that an interstate conflict can be reduced or eliminated through trade.

6. Conclusions and Further Research

In the present analysis, a study of the impact of economic interdependence on interstate conflict was attempted with the use of a sample that consisted of three dyads of countries facing a similar context of interstate conflict: India-Pakistan, Russia-Ukraine and Yemen-Saudi Arabia. The results show that only exports from country 1 to country 2 have an impact on the level of defense expenses either for country 1 or for country 2. This indicates that economic interdependence does not necessarily reduce interstate conflicts, since both countries 1 and 2 increase the defense expenses even though exports from country 1 to country 2 increase. Our contribution in the current literature relies upon the correlation between defense expenses and bilateral trade and is in the direction of the research of Seitz et al. (2015). There has been a big diversity of dependent variables employed in the relevant studies, such as trade expectations (Copeland, 1996), common interests (Li and Sacko, 2002), interaction between domestic politics and the international system (Kapstein, 2003), income ratio (Martin et al., 2008), Preferential Trade Agreements (Herge et al., 2010; Long, 2008), trade (Barbieri and Levy, 1999; Long and Leeds, 2006), Militarized Interstate Disputes (MIDs) (Copeland, 1996; Oneal and Russett, 1999; Gartzke et al., 2001; Powers, 2004; Martin et al., 2008; Li and Reuveny, 2011). As all studies, it has certain limitations that primarily stem from data availability; three dyads where analyzed and certain proxies were used. Consequently the results depend purely on the span of the dataset. Our future research venues include the extension to additional dyads to more variables that are relevant to the interstate conflict as well as the economic interdependence, provided data become available. Furthermore, as indicated by the anonymous reviewers, it is worth investigating whether the strength of defense can affect the mutual trade of two countries. In addition, as recommended by the anonymous reviewers it would be interesting to apply game theoretical approaches in order to establish the hypotheses around economic interdependencies prior to the investigation of the correlation of the latter to the interstate conflict.

## A2: Attribution

### 1NC --- Attribution Impossible

#### Advanced techniques make attribution impossible

Finlay & Payne 19 --- Lorraine Finlay is a lecturer in the School of Law at Murdoch University, Christian Payne is a Lecturer in Computer Science at Murdoch University, “The Attribution Problem and Cyber Armed Attacks”, American Journal of International Law>AJIL Unbound>Volume 113, 24 June 2019, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/attribution-problem-and-cyber-armed-attacks/ADC0F451A9B560D8A070A753E61E874F

There are, broadly speaking, two aspects to the attribution problem. The first is the technical problem of how to identify the true origin of a particular attack and the identity of those who carried it out. The second is the legal question of whether and if so, when, factual attribution allows a state to be held responsible for the cyberattack under international law.

The technical consequences of the unique characteristics of cyberattacks have been widely acknowledged. Dan Efrony and Yuval Shany have highlighted two key differences between cyber and other kinds of attacks: the boundlessness and anonymity of the cyber domain.Footnote11 As cyberspace is not limited by physical or geographical borders, questions of jurisdiction and enforcement become more complex. Perpetrators use various techniques to obscure their true location, and isolating the origin of a cyberattack is extraordinarily difficult when attacks are routed through multiple machines in multiple locations across the world. These techniques make the task of retrospectively establishing a forensic link between an attacker and an incident extremely difficult. They allow cyberattacks to be carried out with little risk to those involved, with perpetrators able to mask their identity and potentially even misattribute blame.

Thus, cyberattacks often take more time to detect and evaluate than traditional kinetic attacks. This analysis might require using classified intelligence and technological capabilities that a state would prefer not to reveal. All of these factors make it challenging to attribute cyberattacks.

These technical difficulties have two main consequences for attribution, both of which are critical in relation to cyber armed attacks. The first is that the risk of misattribution is heightened, leading to the potential for serious conflict escalation if a state mistakenly targets an innocent third party in its self-defense response. The second is that the length of time it will realistically take to correctly identify the perpetrator will very likely mean that it will be significantly harder for a state to satisfy the factors of immediacy and necessity required to lawfully exercise its right of self-defense.

### Ext --- Attribution Impossible

#### Attribution impossible

Fier 21 --- Justin Fier Director for Cyber Intelligence & Analytics at Darktrace, “In Cyberwar, Attribution Can Be Impossible — and That's OK”, October 18, 2021, https://www.darkreading.com/analytics/in-cyberwar-attribution-can-be-impossible---and-that-s-okay

An enemy you can neither see nor identify looms large. But it's time to acknowledge a hard truth: In today's world, attack attribution in cyberspace can be impossible for all but the best-resourced governments and organizations. A recent analysis of more than 200 cybersecurity incidents associated with nation-state activity since 2009 found that half of them involved "low budget, straightforward tools that could be easily purchased on the darknet."

The reality is apparent: We may never know who is behind incidents that create chaos and cause damage in most cases.

#### NATO coop cant overcome the attribution problem

Horowitz 10 --- Michael Horowitz, Assistant professor of political science at the University of Pennsylvania and a senior fellow at the Foreign Policy Research Institute. He has also held fellowships at the Olin Institute for Strategic Studies at Harvard, the Belfer Center for Science and International Affairs at Harvard, and the Weatherhead Center for International Affairs at Harvard. “A Common Future? NATO and the Protection of the Commons”. Transatlantic Paper Series No. 3 October 2010. https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Trans-Atlantic\_Papers\_3-Horowitz.pdf

Cyberspace is also a realm where traditional notions of deterrence may break down. Deterring a threat by issuing counter-threats to deliver a devastating response to any cyber attack against the United States and its NATO allies may seem like an attractive solution to the cyber security challenge. The high costs associated with defending networks from cyber intrusions and the relatively low costs of launching a cyber attack have led many to analogize cyber deterrence to nuclear deterrence.31 However, cyber attacks lack the stable footprint of conventional military forces. The fact that terrorist attacks do not leave a “return address” is accentuated in the case of cyber warfare. In the case of a cyber attack, for example, even tracking down the specific computer from which an attack was launched might not give the attacked country sufficient information to distinguish whether a country, terrorist group, or rogue individual launched an attack from that particular computer. These concerns, in part, are why U.S. Deputy Secretary of Defense William Lynn recently stated that denying adversaries access to U.S. information systems in the first place, rather than planning to retaliate in case of an attack, encompasses the bulk of U.S. defensive efforts.32 The United States and its NATO partners must invest heavily in defending their networks from intrusion and cannot be confident that maintaining nascent retaliatory capabilities will suffice to deter attacks. Furthermore, while strong cyber ties between NATO members might not ensure that deterrence succeeds, weak cyber ties will almost certainly encourage adversaries to launch more cyber incursions against NATO members.33 Finally, since many future wars will likely include major cyber components, thinking about cyberspace as a very separate sphere of warfare delinked from other areas of conflict is counterproductive.34

### 1NC --- Attribution Doesn’t Deter

#### Even successful attribution fails to deter

Sweijs & Zilincik 19 --- Tim Sweijs Director of Research at The Hague Centre for Strategic Studies, and Samo Zilincik, associated research fellow with a new article in the Texas National Security Review, “Report Part Title: Deterrence by Democracies in a Hybrid Context”, Published by: Hague Centre for Strategic Studies (2019), https://www.jstor.org/stable/pdf/resrep24191.6.pdf?refreqid=excelsior%3Aac9305baa499cc4635e8cc7dc28c6da2&ab\_segments=&origin=&acceptTC=1

The opaqueness of hybrid activities typically complicates any deterrent efforts which benefit from transparency and clarity.79 After all, only if actions can be observed by the deterrer and attributed to a particular actor, is it possible - relying on backwards inductive logic - to deter that actor from taking that action in the first place. Hybrid conflict challengers, it is said, can easily circumvent any red lines laid down by the deterrer and rely on plausible deniability for cover.80 Examples that are sometimes pointed at include both the Russian government’s denial that green little men invading the Crimean peninsula were Russian,81 chemical attacks on UK soil, cyberattacks on critical US infrastructure of various origins, and a variety of attempts to manipulate the information domain in various European countries and in North America. But both for traditional and new domains that argument does not necessarily seem to hold up. In fact, as we have seen in many of these cases, the perpetrator either could have been identified or was in fact identified. In other words, attribution took place. Despite Putin’s denial that the green little men invading the Crimean Peninsula were Russian, this was not - or should at least not have been - hard to verify for Western military intelligence services. In the Skripal chemical attacks on British soil in March 2018, the UK government announced within eight days that the toxin was of Russian provenance, and the perpetrators were identified and charged later that year. Attribution in the cyber domain poses more challenges.82 As Joseph Nye explains:

“If [..] attackers do use the Internet, they can mask the point of origin behind the flags of several remote servers, which can be located in a variety of jurisdictions. They can use nonstate actors as proxies and create false flags. … Moreover, knowing the true location of a machine is not the same as knowing the ultimate instigator of an attack.”83

### Ext --- Attribution Doesn’t Deter

#### Attribution won’t stop hybrid attacks

Detlefsen 15 --- MAJ William Detlefsen United States Army. “Cyber Attacks, Attribution, and Deterrence: Three Case Studies”, School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas, 23-05-2015, https://apps.dtic.mil/sti/pdfs/AD1001276.pdf

Cyberspace is a relatively new and poorly understood domain of human activity. Despite the potential for expression, exchange of knowledge, and creation, it quickly became another area for human conflict. These conflicts range from the petty to major state competition for power and resources. To explore the likelihood of deterrence providing some level of stability and peace, this monograph examined three different cyber attacks, the ability for the victims to attribute the attack, the response chosen, and the effect on future cyber attacks.

Across the three different incidents, there are different dynamics at work. The DDoS attack against Estonia was a low-grade nuisance, whose broad attack base supported plausible deniability by a single actor. The Estonian government suspected Russian government involvement, but could not publicly attribute it to specific actors. Even if they could attribute it, there is the question of whether or not the Russian government would have helped stop the attacks. Given the unwillingness of the Russian government to assist in the investigation and the repeated statements that the attacks were simply acts of civil disobedience by concerned patriots, it is unlikely the Russian government would have helped stop the attack.

### 1NC --- NATO Unity D

#### NATO doesn’t solve

Ranhotra 22 --- Sanbeer Singh Ranhotra is a political columnist at TFIPOST, “The irrelevance of NATO is now out in the open” February 25, 2022, https://tfiglobalnews.com/2022/02/25/the-irrelevance-of-nato-is-now-out-in-the-open/

NATO is a headless chicken. It has been reduced into an insignificant entity which when told to shut up by Russia, goes to a corner and quietly sits down – making sure to behave itself. It is quite remarkable how Ukraine thought this organisation would come to its aid in the event of a large-scale Russian invasion. Leave alone military aid, NATO has not even been able to agree on a decisive economic sanctions package that would have an immediate effect on Moscow.

Russia has invaded Ukraine. The world is outraged. The United States and its allies are angry. NATO is infuriated. But here’s the ridiculously painful part: NATO can do nothing but mutely spectate as Russian President Vladimir Putin redefines Eastern Europe. Essentially, NATO has failed. It had one mandate – to protect Europe. It has failed to achieve its primary objective, and this would have lasting consequences for the security alliance.

#### Collapse inevitable

Ranhotra 22 --- Sanbeer Singh Ranhotra is a political columnist at TFIPOST, “The irrelevance of NATO is now out in the open” February 25, 2022, https://tfiglobalnews.com/2022/02/25/the-irrelevance-of-nato-is-now-out-in-the-open/

NATO Will Cease to Exist

The invasion of Ukraine has shown that Europe is not united. Every European country is keeping its interests above the supposed idea of protecting ‘Europe’ as a whole. There is no cohesion among European nations, and Joe Biden’s administration remains simply clueless.

The United Kingdom, meanwhile, is thanking its stars that it left Europe at the right time. But the larger message that this fiasco has sent out has not been lost on any country. Now, every European country knows that NATO – for all purposes – is a toothless organisation.

The crisis in Eastern Europe will lay the foundation for the disintegration and ultimate evaporation of NATO.

### Ext --- NATO Unity D

#### NATO doesn’t solve conflict—just makes war more likely:

MEDEA BENJAMIN, 12/6/2019 (co-founder of CODEPINK for Peace, “Why NATO should be obsolete,” <https://www.salon.com/2019/12/06/nato-should-be-obsolete_partner/>, Retrieved 6/15/2022)

The three smartest words that Donald Trump uttered during his presidential campaign are “NATO is obsolete.” His adversary, Hillary Clinton, retorted that NATO was “the strongest military alliance in the history of the world.” Now that Trump has been in power, the White House parrots the same worn line that NATO is “the most successful Alliance in history, guaranteeing the security, prosperity, and freedom of its members.” But Trump was right the first time around: Rather than being a strong alliance with a clear purpose, this 70-year-old organization that is meeting in London on December 4 is a stale military holdover from the Cold War days that should have gracefully retired many years ago. NATO was originally founded by the United States and 11 other Western nations as an attempt to curb the rise of communism in 1949. Six years later, Communist nations founded the Warsaw Pact and through these two multilateral institutions, the entire globe became a Cold War battleground. When the USSR collapsed in 1991, the Warsaw Pact disbanded but NATO expanded, growing from its original 12 members to 29 member countries. North Macedonia, set to join next year, will bring the number to 30. NATO has also expanded well beyond the North Atlantic, adding a partnership with Colombia in 2017. Donald Trump recently suggested that Brazil could one day become a full member. NATO’s post-Cold War expansion toward Russia’s borders, despite earlier promises not to move eastward, has led to rising tensions between Western powers and Russia, including multiple close calls between military forces. It has also contributed to a new arms race, including upgrades in nuclear arsenals, and the largest NATO “war games” since the Cold War. While claiming to “preserve peace,” NATO has a history of bombing civilians and committing war crimes. In 1999, NATO engaged in military operations without UN approval in Yugoslavia. Its illegal airstrikes during the Kosovo War left hundreds of civilians dead. And far from the “North Atlantic,” NATO joined the United States in invading Afghanistan in 2001, where it is still bogged down two decades later. In 2011, NATO forces illegally invaded Libya, creating a failed state that caused masses of people to flee. Rather than take responsibility for these refugees, NATO countries have turned back desperate migrants on the Mediterranean Sea, letting thousands die. In London, NATO wants to show it is ready to fight new wars. It will showcase its readiness initiative—the ability to deploy 30 battalions by land, 30 air squadrons and 30 naval vessels in just 30 days, and to confront future threats from China and Russia, including with hypersonic missiles and cyberwarfare. But far from being a lean, mean war machine, NATO is actually riddled with divisions and contradictions. Here are some of them: French President Emmanuel Macron questions the U.S. commitment to fight for Europe, has called NATO “brain dead” and has proposed a European Army under the nuclear umbrella of France. Turkey has enraged NATO members with its incursion into Syria to attack the Kurds, who have been Western allies in the fight against ISIS. And Turkey has threatened to veto a Baltic defense plan until allies support its controversial incursion into Syria. Turkey has also infuriated NATO members, especially Trump, by purchasing Russia’s S-400 missile system. Trump wants NATO to push back against China’s growing influence, including the use of Chinese companies for the construction of 5G mobile networks—something many NATO countries are unwilling to do. Is Russia really NATO’s adversary? France’s Macron has reached out to Russia, inviting Putin to discuss ways in which the European Union can put the Crimean invasion behind it. Donald Trump has publicly attacked Germany over its Nord Stream 2 project to pipe in Russian gas, but a recent German poll saw 66 percent wanting closer ties with Russia. The UK has bigger problems. Britain has been convulsed over the Brexit conflict and is holding a contentious national election on December 12. British Prime Minister Boris Johnson, knowing that Trump is wildly unpopular, is reluctant to be seen as close to him. Also, Johnson’s major contender, Jeremy Corbyn, is a reluctant supporter of NATO. While his Labour Party is committed to NATO, over his career as an anti-war champion, Corbyn has called NATO “a danger to world peace and a danger to world security.” The last time Britain hosted NATO leaders in 2014, Corbyn told an anti-NATO rally that the end of the Cold War “should have been the time for NATO to shut up shop, give up, go home and go away.” A further complication is Scotland, which is home to a very unpopular Trident nuclear submarine base as part of NATO’s nuclear deterrent. A new Labour government would need the support of the Scottish National Party. But its leader, Nicola Sturgeon, insists that a precondition for her party’s support is a commitment to close the base. Europeans can’t stand Trump (a recent poll found he is trusted by only 4 percent of Europeans!) and their leaders can’t rely on him. Allied leaders learn of presidential decisions that affect their interests via Twitter. The lack of coordination was clear in October, when Trump ignored NATO allies when he ordered U.S. special forces out of northern Syria, where they had been operating alongside French and British commandos against Islamic State militants. The U.S. unreliability has led the European Commission to draw up plans for a European “defense union” that will coordinate military spending and procurement. The next step may be to coordinate military actions separate from NATO. The Pentagon has complained about EU countries purchasing military equipment from each other instead of from the United States, and has called this defense union “a dramatic reversal of the last three decades of increased integration of the transatlantic defence sector.” Do Americans really want to go to war for Estonia? Article 5 of the Treaty states that an attack against one member “shall be considered an attack against them all,” meaning that the treaty obligates the U.S. to go to war on behalf of 28 nations—something most likely opposed by war-weary Americans who want a less aggressive foreign policy that focuses on peace, diplomacy, and economic engagement instead of military force. An additional major bone of contention is who will pay for NATO. The last time NATO leaders met, President Trump derailed the agenda by berating NATO countries for not paying their fair share, and at the London meeting, Trump is expected to announce symbolic U.S. cuts to NATO’s operations budget. Trump’s main concern is that member states step up to the NATO target of spending 2 percent of their gross domestic products on defense by 2024, a goal that is unpopular among Europeans, who prefer that their tax dollars go to nonmilitary items. Nevertheless, NATOSecretary-General Jens Stoltenberg will brag that Europe and Canada have added $100 billion to their military budgets since 2016—something Donald Trump will take credit for—and that more NATO officials are meeting the 2 percent goal, even though a 2019 NATO report shows only seven members have done so: the U.S., Greece, Estonia, the UK, Romania, Poland and Latvia. In an age where people around the world want to avoid war and to focus instead on the climate chaos that threatens future life on earth, NATO is an anachronism. It now accounts for about three-quarters of military spending and weapons dealing around the globe. Instead of preventing war, it promotes militarism, exacerbates global tensions and makes war more likely. This Cold War relic shouldn’t be reconfigured to maintain U.S. domination in Europe, or to mobilize against Russia or China, or to launch new wars in space. It should not be expanded, but disbanded. Seventy years of militarism is more than enough.

#### NATO is obsolete—not necessary to solve conflict.

Christian Whiton, 7/6/2018 (State Department senior advisor in the Donald Trump and George W. Bush administrations, “NATO Is Obsolete,” <https://nationalinterest.org/feature/nato-obsolete-25167>, Retrieved 6/15/2022)

Despite endless searches for a new mission to justify its massive burden on U.S. taxpayers, NATO has failed to be of much use since then. As its boosters like to remind us, after 9/11, the alliance invoked its Article 5 mutual-defense provision on our behalf. But action from America’s allies did not follow the grandiose gesture—the NATO mission in Afghanistan relied mostly on U.S. forces and effectively failed. Today, the alliance’s bureaucrats and some member states spotlight a threat from Russia as a reason for keeping the organization alive, along with a laundry list of “train and equip” missions. Yet NATO members' defense budgets don't reflect a real sense of danger from Russia or anyone else. Among the twenty-nine members, only the United States is really serious about its Article 3 obligations to defend itself, spending approximately $700 billion or 3.5 percent of its GDP on defense. No other NATO member comes close to this proportion, and the vast majority fail even to meet the modest, self-imposed requirement to devote at least 2 percent of GDP to defense. Britain and Poland are rare members that meet the 2 percent requirement. One of the worst free-riders is Canada, which spends just 1 percent of its GDP on security, amounting to $20 billion. Furthermore, Germany spends a similarly pathetic 1.2 percent. Compare that to non-NATO members facing real threats, some of which spend 5-10 percent of their GDPs on defense. These include Saudi Arabia and the United Arab Emirates, who must contend with Iran and spend nearly a combined $100 billion. Israel, which faces the same enemy, adds $15 billion to the equation. Despite protestations of poverty at a time when their economies have never been larger, NATO members are more than willing to rack up additional liabilities, knowing America has their back. Last year, the alliance welcomed Montenegro. It is now poised to admit the Former Yugoslav Republic of Macedonia, which would mean the United States is pledged to defend a nation that devotes just $120 million per year to its own defense, not quite as much as the Cincinnati Police Department. But the reality is there is no truly capable Russian foe seriously threatening the West. Russia has one million uniformed personnel in its military, the world’s second-largest behind America, but the European Union could easily afford to match that with its combined $17 trillion economy—ten times larger than Russia’s. However, it needn’t bother as Moscow spends just $61 billion on its overwrought military, which doubles as an employment program. Russia’s Vladimir Putin has gotten the most from Russia’s military, occupying parts of Georgia and Ukraine and gaining influence in Syria by backing the Assad regime. Still, his success in all three cases rested heavily on surprises that Moscow seems unlikely to be able to repeat against prepared and adequately funded European militaries. Yer we should expect to hear none of this nuance at the NATO summit, as poohbahs of the dying old European political order gather to tut-tut President Trump in the alliance’s fancy new $1.4 billion headquarters, funded predominantly by American taxpayers. To get out of this abusive relationship, Trump should begin the process of limiting America's role in NATO. A good model is that of Sweden, which cooperates with NATO on some matters and not on others. Such an approach could allow joint training, but end the practice of having over-burdened U.S. taxpayers foot the bill for wealthy Europeans' security. As part of this plan, Trump could mothball U.S. bases in Europe and shift most resources spent there and in the Atlantic to the Indo-Pacific region, where China and Iran pose real threats to America—and against which NATO is irrelevant. Europe is prosperous and treats America like a patsy. Let it stand on its own.

#### Alliance is resilient, but fails

Gowan 15 – Richard Gowan, Research Director at New York University’s Center on International Cooperation and Senior Policy Fellow at the European Council on Foreign Relations, “U.S. to Europe: Don’t Go Soft on American-Led Global Order”, World Politics Review, 3-16, http://www.worldpoliticsreview.com/articles/15297/u-s-to-europe-don-t-go-soft-on-american-led-global-order

The United States sent its European allies some stern signals about their obligations to the American-led international order last week. On Monday, U.S. Ambassador to the U.N. Samantha Power visited Brussels, where she warned NATO members to halt their “dangerous” defense cuts and called on European powers to offer more troops to United Nations peace operations. Power argued that European armies, which currently provide less than 10 percent of all U.N. peacekeepers worldwide, could have a “momentum-shifting” impact on beleaguered blue helmet missions in trouble spots such as South Sudan. Instead, she underlined, “European countries have drawn back from peacekeeping,” while the European Union has shied away from high-intensity missions. This was an accurate but uncomfortable message for EU and NATO members, whose appetite for stabilization missions remains very low after their Afghan nightmares. Power emphasized threats from the Middle East and North Africa to bolster her argument. Later in the week, anonymous U.S. officials sent a reminder that they expect European assistance in Asia, too. This time, the sore point was economic cooperation rather than military affairs. Washington has taken umbrage at Britain’s decision to invest in the Asian Infrastructure Investment Bank (AIIB), a new organization proposed by China to offset the U.S.-backed Asian Development Bank. A U.S. source told the Financial Times that the U.K. seemed to be adopting a stance of “constant accommodation of China.” British journalists seemed shocked that the U.S. might question Washington’s “special relationship” with London. In reality, the relationship has been on the rocks for some time, as U.S. President Barack Obama’s administration has worked out thorny but productive alternative relationships with Paris and Berlin on political, security and economic matters. Yet the U.S. criticism of the U.K. involvement with the AIIB revealed a deeper concern about potential challenges to U.S. leadership in the international system—and Europe’s commitment to sustaining American primacy in particular. The current multilateral system rests on two basic pillars. The first of these is a U.S. political commitment to work through international institutions, even if this is often more a matter of rhetoric than reality. The second is the continued willingness of Western European governments and Japan to pay a large chunk of the costs of this system, in addition to backing the U.S. against challengers such as Russia and China. This has never been an entirely stable set-up. It has most obviously broken down over individual crises such as the 2003 Iraq War, when France and Germany lined up with China and Russia to oppose the U.S.-led invasion. More fundamentally, it has been clear ever since the long process of decolonization brought waves of Asian and African states into the U.N. and other international institutions in the 1950s and 1960s that the “global order” could not rest on a trans-Atlantic bargain indefinitely. It has nonetheless proved to be a remarkably durable arrangement. The U.S., EU members and Japan combined continue to pay nearly 80 percent of the U.N.’s main budget. Their shared grip on the institution remains powerful. Non-Western powers have invested in elements of the international system: China has aimed to expand its limited role in the International Monetary Fund, while Arab countries have focused on humanitarian aid in response to the crises in their neighborhood. But the overall U.S. and European dominance of these institutions is extremely hard to break. The benefits to Western policymakers are also clear. Non-Western officials at the IMF believe that the fund has been far too deferential to the EU over the eurozone crisis, even if the European Commission has at the same time argued that the IMF has been unduly critical of EU efforts. In the meantime, close observers of the U.N. believe that Britain, France and the U.S. are now actually more powerful in the Security Council than they were 10 to 15 years ago, despite collisions with Russia and China over matters such as Syria, as they have consolidated their powers to draft resolutions and control the organization’s peace operations and sanctions regimes. The Obama administration, with its emphasis on building relations with non-Western powers, seemed intent on challenging this state of affairs. It did so to some extent in its early years. Washington ganged up with Asian governments in the G-20 to impose IMF reforms that were meant to reduce European leverage in the organization, although the measures have subsequently been held up in the U.S. Congress. Obama’s team also tried to show greater sensitivity to Russia’s positions on crises like Syria than previous U.S. administrations. But the U.S. has failed to re-engineer international cooperation. Russia remains obstreperous, and China seems more interested in developing new organizations, such as the AIIB, than investing in existing U.S.-led bodies. Episodes such as the 2011 Libyan war, when Beijing and Moscow waved through the Western intervention and then went on to slam it, have left doubts about the chances of putting international institutions on a new political footing. Having looked for better partners elsewhere, the U.S. is stuck with Europe. And yet Europeans seem to be distinctly reluctant to play along. NATO countries appear likely to respond to Power’s plea and do a bit more for peacekeeping in the near future, as the Netherlands and Nordic countries have recently done in Mali. But “stay at home-ism” is still a credible power doctrine for some members of the alliance. Meanwhile, most EU members, with honorable exceptions such as Sweden and the U.K., severely cut their development and humanitarian budgets during the financial crisis. In economic terms, no EU member can afford to ignore China’s wealth and markets. So the European pillar of the international system looks very weak indeed. This does not mean that it is about to crack. European policymakers are not about to dump Washington, and they still take its criticisms to heart, as the attention given to Power’s speech demonstrates. If China’s ambassador to the U.N. gave a speech in Brussels, it would very likely go unnoticed. But the U.S. has to assume that, at best, European governments are going to be less consistent and predictable supporters of the post-1945 multilateral system—and that the system as a whole will suffer as a result.

#### No impact---NATO’s ineffective.

Christopher **Roach 18**. Attorney and commentator in The Federalist, the Washington Legal Foundation, the Marine Corps Gazette, and the Orlando Sentinel. 07-16-2018. “What Good Is NATO?,” https://amgreatness.com/2018/07/16/what-good-is-nato/

NATO’s weakness stems not only from dubious grand strategy, but also from its limited practical value. Consider the Libyan Campaign. No longer Europe’s hour, NATO’s member states aligned with one another to persuade the U.S. to join a dubious campaigns, where highfalutin rhetoric of human rights masked realpolitik concerns for things like oil. The NATO tail ended up wagging the American dog, and the U.S. military had to make up for key NATO deficiencies in logistics, electronic warfare, surveillance, and airpower. In the end, the NATO allies worked together and toppled Qaddafi, but the place fell apart, jihadis exploited the ungoverned space, a U.S. ambassador was killed, and the campaign did little to contribute to U.S. or European security interests. A paragon of the managerial class, Hillary Clinton summed it up with her callous retort: “What difference at this point does it make?” Libya is not the exception. In Bosnia and Kosovo, NATO’s European members repeatedly have shown very meager power projection capabilities. In Afghanistan, where many of our NATO allies assisted our campaign after the 9/11 attacks under NATO’s Article 5, individual NATO participants often operated under wildly different rules of engagement, limiting the effectiveness of various nations’ contingents. While there are common standards across NATO, ties of history and friendship, as well as a common Western culture, it’s not so clear that these factors have ever overcome the divergent abilities of NATO members when called to action. In short, as it has expanded its membership and its mission, NATO has become less effective. And, to the extent it is effective at all, the United States has always had to do most of the work.

**NATO’s cyber policy is flexible and in sync now**

**Brent 19** --- Laura Brent currently serves in NATO’s Emerging Security Challenges Division and has previously held cyber policy roles in both the public and private sectors, addressing complex strategy, policy and operational challenges in varied and fast-changing environments. 2-12-2019. “NATO’s role in cyberspace.” https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

Cyberspace as a domain of operations

Since the Allies recognised cyberspace as a **domain of operations** in 2016, NATO has achieved several **important milestones**. Perhaps most notably, in October 2018, NATO announced the initial stand up of the **Cyberspace Operations Centre**, or CyOC, in its trial structure. The CyOC serves as NATO’s **theatre component** for cyberspace and is responsible for providing cyberspace **situational awareness**, **centralised planning** for the cyberspace aspects of Alliance operations and missions, and **coordination** for cyberspace **operational concerns**.

Along with this critical organisational adaptation, Allies **agreed** at the Brussels Summit how to **integrate** sovereign cyber effects, provided **voluntarily** by Allies, into Alliance **operations** and **missions**. This is **fully coherent** with NATO’s **defensive mandate**, as it aligns how NATO **defends itself in cyberspace** as it does in other domains, with Allies contributing tanks, planes, and ships to Alliance operations and missions.

**Strategy** and **guidance** is also maturing. In June 2018, Allies **approved** the **V**ision and **S**trategy on **C**yberspace as a **D**omain of **O**perations. It is anticipated that, in 2019, NATO’s first cyberspace operations doctrine will be completed, subject to Allied approval, which will provide guidance to NATO commanders.

These structures and concepts are only of value if implemented and put to use. To this end, NATO is **adapting** its **education**, **training**, and **exercising** programmes. The **NATO C**ooperative **C**yber **D**efence **C**enter of **E**xcellence has been given responsibility for **identifying** and **coordinating** education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

Every year, Cyber Coalition, NATO’s **biggest** and **most important** cyber defence exercise, involves more than **700 participants** from NATO Allies, partner countries, the European Union, industry and academia. © NATO

Cyber-specific exercises are being **continually updated** in light of **changed policy** and **doctrine**. In 2018, Cyber Coalition – NATO’s **flagship** cyber defence exercise with more than 700 participants from Allies, partners and NATO – exercised the **integration** of sovereign cyber effects **voluntarily provided** by an Ally. Other NATO exercises, such as the Crisis Management Exercise (aimed at NATO Headquarters) and Trident Juncture 2018 (aimed at the entire military chain of command), have and will continue to include more robust cyber scenarios.

### 1NC --- Hybrid Ward D

**NATO response will always be proportional**

**NBC 10** --- NBC News, Red Tape, “Could cyber skirmish lead U.S. to war?”, June 2010, https://www.nbcnews.com/business/consumer/could-cyber-skirmish-lead-u-s-war-flna6C10406234

Imagine this scenario: Estonia, a NATO member, is cut off from the Internet by cyber attackers who besiege the country's bandwidth with a devastating denial of service attack. Then, the nation's power grid is attacked, threatening economic disruption and even causing loss of life as emergency services are overwhelmed. As international outcry swells, outside researchers determine the attack is being sponsored by a foreign government and being directed from a military base. Desperate and outgunned in tech resources, Estonia invokes Article 5 of the NATO Treaty -- an attack against one member nation is an attack against all. It requests an immediate response from its military allies: Bomb the attacker's command-and-control headquarters to stop the punishing cyber attack.

Now, the U.S. government is faced with a chilling question: Should it get dragged into a shooting war by a cyber attack on an ally? Or should it decline and threaten the fiber of the NATO alliance?

About half this fictionalscenario **occurred in 2007**, when Estonian government and financial Web sites were ~~crippled~~ [knocked out] by a cyber attack during a dispute with Russia. **That incident never escalated** to this hypothetic level, however: The source of the attack was unclear, physical harm did not occur and **Estonia never invoked Article 5.**

The incident did, however, get other NATO members thinking: When would they be required to rise to the defense of an ally during a cyber attack?

Last year, a working group led by former U.S. Secretary of State Madeline Albright was formed by NATO to study the future of the alliance in a post Cold War world. When the group issued its report last month, aimed at helping NATO form a new "Strategic Concept," the thorny issues raised by cyber war were listed as one of the three toughest challenges facing the alliance. NATO is expected to approve the Strategic Concept this November during a meeting in Lisbon, and cyber war issues will be hotly debated.

Mutual defense is the heart of the NATO alliance, formed in 1949 in the wake of World War II, largely to combat the aspirations of an expanding Soviet Union. Article 5 lays out the obligations of members in plain language:

"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them ... will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."

Despite all the attention Article 5 has received during the 60-plus years of NATO, it has been invoked only once -- after the 9/11 attacks. That led to an alliance attack to remove the Taliban from power in Afghanistan.

That means the odds of a rudimentary botnet attack against a NATO member leading to war **are quite small.** They are not zero, however. The Albright group's report, titled "NATO 2020," was stark in its assessment -- ignoring the issue would probably only encourage attackers.

"The next significant attack on the Alliance may well come down a fiber optic cable," it reads. "A cyber attack that leads to chaos in one city may inspire copy-cat criminals in another. Due to the reach of modern media, even terrorist groups and pirate bands now have public relations specialists and NATO, when and wherever it acts (or fails to act), will do so with a global audience."

Among the report's recommendations(PDF): Give NATO military leaders pre-delegated authority to respond "in an emergency situation such as a missile or cyber attack."

'What is the threshold for crossing the cyber line?'

Roger Cressey, a former member of the U.S. National Security Council, said there is a long list of unanswered questions that NATO hasn't begun to resolve.

"If there is a cyber attack, does NATO respond in kind? Do the NATO allies with the most advanced cyber capabilities respond on behalf of the member that was attacked?" wondered Cressey, now a consultant with Good Harbor Consulting and an NBC analyst. "Should a response be limited only to cyberspace or should kinetic options be on the table too? This raises some very important issues -- do you attack another country with missiles and aircraft in response to a cyber attack? What is the threshold for crossing the cyber line and into physical responses?"

An even thornier issue, he said, is "attack attribution." As was the case of the Estonian attacks and more recent attacks on Google and other big tech companies, it's often difficult to positively identify cyber-attackers. So foreign governments or other enemies can easily blame cyber attacks on rogue groups.

"Doctrine on cyber attack is a very problematic issue, one that the Pentagon is struggling with right now," Cressey said. "If individual countries haven't figured it out yet, then it's a guarantee that collective defense entities like NATO will be even further behind in coming up with an agreed upon approach."

NATO lawyer: A high bar

Lawyer Eneken Tikk is in a unique position to understand the nuances of the Article 5 mutual defense debate. She is the acting policy chief at a NATO training center called the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, which was founded in 2008 in the wake of the 2007 cyber attack. She believes there is undoubtedly a legal basis for a mutual defense response to a cyber attack -- **but the threshold for invoking** such a response **is very high**. For starters, she said, mere electronic disruptions probably **wouldn't clear the bar**. Involving other NATO nations would require "a cyber attack on a country's power networks or critical infrastructure (**that) resulted in casualties** and destruction **comparable to an armed attack,"** she said.

**And even casualties might not trigger treaty obligations**, she said.

"There is no clear threshold of a cyber armed attack - and even a kinetic attack is not always what the U.N. Charter considers as a threshold for invoking the right to individual (or collective) self-defense," she said. She pointed to research that suggests an attack "has to be of enough scope, duration and intensity ... to satisfy the accepted criteria of an armed attack under international law." Neither an overnight border skirmish nor a troublesome but temporary denial of service attack would qualify, she suggested. **That why the Estonian government did not invoke Article 5 in 2007, she said.**

The Albright report makes allowances for all these gray areas, but hints at a formula it suggests could be put in place to arrive at more delicate decisions.

"There is, of course, nothing ambiguous about a cross border military assault by the combined armed forces of a hostile country," it said. "However, there may well be doubts about whether an unconventional danger -- such as a cyber attack or evidence that terrorists are planning a strike -- triggers the collective defense mechanisms of Article 5. In the event, this will have to be determined by the ... nature, source, scope and other aspects of the particular security challenge."

'Can a cyber attack invoke a physical response?'

Mark Rasch, former head of the Justice Department's computer crimes unit and now a consultant at Secure IT Experts, said that NATO's attempt to clarify members' obligations during cyber attack is further complicated by the fact that low-level cyber attacks are happening **constantly**. Some are better described as espionage or spying than cyber war, and many come from corporations or curious kids. On the other hand, some of those "curious kids" are state-sponsored, he said.

"We've been having low-level cyber **for 30 years**," Rasch said. "There's been penetration testing, Web defacements, denial of service attacks, propaganda attacks. But we haven't yet had a cyber attack where a nation-state mobilizes to attack the critical infrastructure of another nation."

**Hybrid deterrence high**

**Rynning 20** --- Sten Rynning is Professor of War Studies and Vice Dean for Research at the faculty of business and social sciences, the University of Southern Denmark (SDU) in Odense, Denmark, “Deterrence in the 21st Century—Insights from Theory and Practice,” NL ARMS Netherlands Annual Review of Military Studies, 2020, https://library.oapen.org/bitstream/handle/20.500.12657/43303/2021\_Book\_NLARMSNetherlandsAnnualReviewO.pdf

Deterrence by denial (i.e., an ability to deny Russian objectives by defensive measures) is only possible for NATO at the lower rungs of this ladder, and NATO has not been idle here either. In fact, most of the early measures taken by NATO in response to the annexation of Crimea fall into the deterrence of denial category and centre on rapid reaction capacities, especially in the shape of a NATO Response Force (NRF) upgraded for deterrence purposes. The NRF now has a **reinforced**, quicker spearhead—a Very High Readiness Joint Task Force potentially up to 13,000 troops strong, and then two complementing brigades with support (each 13,000 strong) forming a layered, sizeable reaction force explicitly linked to **collective defence** purposes and regularly exercised in Eastern Europe and the Baltic states.35 In 2016, in response to the foreseeable difficulties of projecting mainly Western forces into zones of conflicts close to Russia, NATO decided to established an “enhanced forward presence”—four multinational battalion-sized battle groups —in the Baltic states and Poland, and a “tailored forward presence”—mainly naval forces—in the Black Sea region. Whether these forces can credibly “deny” Russian objectives in the case of limited war is a bone of contention. Most observers and sometimes NATO itself employ the descriptor “tripwire” to these forces, thus indicating that they are triggers that promise to unleash NATO’s big guns and therefore part and parcel of deterrence by punishment. However, US diplomats (interviewed on background) feel more confident that the US battalion embedded (in Poland) in the collective forward presence posture would actually be able to fight and survive, and thus **deny Russian objectives**. That may be so, in which case the conclusion is that NATO has a moderate-to-low—and geographically focused—capacity for deterrence by denial and then a more general and impressive capacity for deterrence by punishment. NATO’s **unquestionable capacity for deterrence** by denial is rather found at the **level of grey zone**, non-kinetic conflict. In this regard, NATO has **upgraded** not only its **cyber defences** and enhanced intelligence coordination, as mentioned, but has **enhanced coordination** with the European Union on hybrid threats, with a 2016 joint declaration leading to a common work program and a collaborative Centre of Excellence for Countering Hybrid Threats, located in Helsinki, the 2016 adoption of societal resilience benchmarks that, while mostly falling outside NATO’s political-military remit, nations must meet, and finally the decision in 2018 to organize counter-hybrid support teams that can tailor assistance to individual allies and circumstances.36 NATO’s full range of actions in response to Russia’s 2014 annexation of Crimea —a range to which this brief overview can do only limited justice—thus combines deterrence by denial (grey zone conflict, societal resilience, reaction and forward deployed forces to counter limited land grabs) and deterrence by punishment (the full chain of reaction and deployable forces, from conventional to nuclear). NATO’s strong suit is the military piece of this posture, but it has considerably adapted to grey zone conflict scenarios in an effort to achieve a **comprehensive deterrence** posture vis-à-vis Russia’s unified (kinetic and non-kinetic) and uninterrupted (all domains, in war and peace) doctrine of “new generation warfare”.

**Hybrid war doesn’t spillover to kinetic conflict**

Jyri **Raitasalo 19**, military professor of war studies at the Finnish National Defence University, 2/3/19, “The Hidden Benefits of Great-Power Conflict with China and Russia,” https://nationalinterest.org/print/feature/hidden-benefits-great-power-conflict-china-and-russia-42932

The fact that practically all serious security threats facing the West have **moved to the gray zone** is a **positive thing**. This means that most—if not all—threats that the western states are confronting are **nonmilitary** in nature. This development has reduced the probability of war breaking out between western states and their adversaries. This is a new development as many western states have overused their militaries during the post–Cold War era to the detriment of other tools of statecraft.

“**Gray-zone conflicts**,” “**hybrid warfare**,” “political warfare” and “competition short of armed conflict” have become mainstream ways to frame and conceptualize contemporary threats facing the United States and its allies and partners in Europe. The western outlook to gray-zone conflicts accentuates daily dangers which over time corrode western shared understandings, narratives and institutions. According to the western reading of the situation, the tools at the disposal of today’s gray-zone actors vary from **info**rmation **war**fare specialists to internet troll farms and offensive cyber actors.

One key theme which unites many gray-zone conflict oracles is the focus on nonmilitary tools with malign intent. As the Secretary-General on NATO Jens Stoltenberg noted already in 2015, “Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and nonmilitary means to stabilize countries. Others use it to destabilize them.” As Stoltenberg noted in his speech, the combination of military and nonmilitary tools to advance one’s interests dates back thousands of years. Why, then, are we so surprised by the fact that Russia and China—and perhaps some other significant actors as well—are conceptualizing, formulating and executing their security strategies in a way that assigns importance to military and nonmilitary tools? Moreover, how come we are surprised by the fact that the **overt use of military force** is seen by Russia and China something that **should be avoided?** Isn’t it smart for any actor to achieve its goals without recourse to the use of large-scale violence? Being able to achieve one’s goals with diplomatic, information, economic, financial, intelligence and law enforcement tools without the use of military force—using all other means than the military within the DIMEFIL model—is a result that **should be commended**. It is a goal that any smart actor within the international system should strive to do.

Today’s international system is competitive. This is a fact. But it has been **competitive for almost all known history of human beings** and the social groups they have formed. From an international security perspective, the two decades of the post–Cold War era—roughly between 1989/1991–2013—were an extraordinary time. During this period the West—North America and Europe—faced no serious security threats in the military or nonmilitary spheres. It was a time of “the unipolar moment” and supposedly “the end of history.” It was during this period that an expanding NATO made a paradigm change by neglecting Article 5 and going out-of-area in search of a new mission. The United States led the way by going “abroad in search of monsters to destroy”—from Somalia, Haiti and Bosnia to Afghanistan, Iraq and Libya. And soon enough, many western states had their hands full of real hard security threats—if not against the states themselves, at least against their deployed troops in operations. During this time, in a matter of two decades, many western states used military force loosely outside of Europe trying to manage almost irrelevant security problems with air power, precision weapons, first-class intelligence, surveillance, and reconnaissance (ISR) technology and—ultimately—by deploying ground troops for counterinsurgency warfare without clearly stated political goals or any significant chance of success. For years sunk costs mattered more than potential future “victory” when western states deliberated new rotations of forces to these operations. Bosnia, Kosovo, Afghanistan and Iraq have defined the western approach to international security and strategy for more than two decades. Continuously ongoing warfare, operations and campaigns somewhere “out there” have become a normal state of affairs—“the new normal” within the West.

Thus, during the two decades of the immediate post–Cold War era, western states redefined their take on international politics, international security and war. This happened at a time, when western (read: American) power had reached its zenith. This time was really an aberration in the long history of relations between states. Unfortunately for the West today, past formulations of security and military operations were based on shaky—even faulty—foundations. They were based on wishful thinking and overtly optimistic future projections about the ability of western states to remain at the top of the international pecking order of state power without being challenged by anyone, anywhere at any time. It was during these two decades that the collective western delusion about the new “rules of the international security game” emerged. And based on this delusion, many western states reformulated their defense policies and national military forces. As we have witnessed during the post–Cold War era, many western states—led by the United States—have intervened in the affairs of other states militarily to an unprecedented degree. Many political problems have been securitized and militarized—seen to require military responses.

The overtly expansive and even militaristic security policy orientation that developed and matured within the West during the post–Cold War era has now collided with very traditional great-power outlook of Russia and China. Although the military power at the disposal of the **U**nited **S**tates has suffered from almost two decades of constant warfighting, it is still second to none, and continues to be for a long time. However, the policies of Russia and China have turned out to be at odds with the definition of international security that was fostered by the western states during the post–Cold War era. The western-dominated international security agenda is not accepted by Russia or China. And due to long-term efforts to strengthen their military forces, Russia and China today need to be taken seriously. For the West, it is unfortunate that the best way for Russia and China to increase their power position and standing in international politics is to attack the existing western-generated internationals security order and its rules of the game. And the easiest way to do this is to use all tools of statecraft—although **scarcely relying on the use of military force**. The overt use of military force reflects the failure to influence others with other—more “economical” tools.

**Supposedly**, China and Russia have been operating—even waging war—below the radar for years now. I argue that many western radars have been **wrongly calibrated** during the post–Cold War years. It is precisely the “noise” in international politics that states should be concerned about. War is—and should be—an aberration. Other methods of statecraft are—and should be—constantly used in order to achieve politically defined outcomes. Radars calibrated only for high-intensity military threats and warfare leaves western statesmen equipped with meager tools to advance their interests.

Much of the western gray-zone talk has been caused by the surprise that Russia’s action in Europe and China’s actions in Asia have caused. Suddenly, during the early years of this decade, states within the western security community were not able to define the rules of the international security system on their own terms. Indeed, the actions of Russia and China have made the return of great-power politics very visible within the international system. It is understandable that the loss of the international pole position has caused distress and anger within the West. But putting things into perspective, it would be hubristic to assume that for an extended period of time western states could have exclusive rights to delineate the logic and rules of international security. Today it is obvious that **the unipolar moment is over. The sooner that this sinks in, the better**. Realizing this is a prerequisite for devising policies that can serve western security interests.

The western discourse on the negative or threatening aspects of the ongoing Russian and Chinese gray-zone **op**eration**s** is based on a **faulty understanding of statecraft or grand strategy**. After all, grand strategy can be understood as a “collection of plans and policies that comprise the state’s deliberate effort to harness political, military, diplomatic, and economic tools together to advance that state’s national interest.” Grand strategy thus reconciles aspirations or ends with means. As we have seen during the last two decades, in most cases the use of military force serves the national interest poorly. Not only does the use of overt violence mobilize active resistance, it also practically in all cases also leads to unintended consequences that are difficult, if not impossible, to manage. What we in the West call gray-zone conflicts or “hybrid warfare” is, in fact, Russia and China advancing their national interests with **normal**—albeit not always with benign—**tools of statecraft**. The presupposition that international relations are always benevolent in nature (as they were for some years after the end of the Cold War—at least for the western states), and that great powers of the day refrain from using malign tools of statecraft when seeking to fulfill their national objectives would be **naïve at best—dangerous at worst**. We should be **pleased** with the fact that China and Russia are highly focused on the **tools below warfare**. This **makes war between Russia or China and the West more unlikely**. Thus, **gray-zone competition is a good thing**. Competition is a normal feature of international politics.

**No military response**

Michael **Rühle 19**, M.A. Degree in Political Science from the University of Bonn, Volkswagen-Fellow at the Konrad-Adenauer-Stiftung and Visiting Fellow at the Center for Strategic and International Studies, “NATO’s Response to Hybrid Threats”, National Institute for Public Policy, 11/4/2019, https://www.nipp.org/2019/11/04/ruhle-michael-natos-response-to-hybrid-threats/

The Role of Military Means

First and foremost, the role of military means in deterring or defending against hybrid attacks is still not fully understood. If certain hybrid actions such as cyberattacks, “fake news” campaigns or interference in elections are to become a permanent component of interstate competition, the role of military deterrence is **likely** to **remain small**. Military means would serve primarily to ensure that a hybrid conflict does not turn into a military conflagration. If, on the other hand, hybrid attacks were only a precursor to a military attack, as was the case in Ukraine in 2014, the defender might have to deploy his military assets earlier.[3] While it may seem **unlikely** that NATO would respond **kinetically** to a hybrid, **non-kinetic** attack and thus be the first to cross the threshold of using armed force, it is important that allies have a firmer grasp of the military and non-military response options. Determining when and how to respond to a hybrid campaign may well turn out to be one of NATO’s toughest challenges in the years ahead. In any case, the mere assertion that more military muscle also produces more deterrence against hybrid warfare is clearly insufficient.

### Ext --- Hybrid War D

**Hybrid tactics fail**

**Lanoska 20** [Alexander Lanoszka, Assistant Professor of International Relations at the University of Waterloo, "Thank goodness for NATO enlargement", 4/7/20, https://link.springer.com/content/pdf/10.1057/s41311-020-00234-8.pdf]

Even the use of so-called **hybrid tactics** may have **limited efficacy** in the Baltic region. The three Baltic countries have been subject to an intense Russian disinformation campaign since at least 2014. **Nevertheless**, local public opinion remains **largely supportive of NATO** and other defense policy measures aimed at boosting deterrence. One reason why these societies may be inoculated against Russian disinformation is that they have gr**own accustomed to seeing Russia in adversarial terms,** thus making average citizens **critical** of pro-Kremlin narratives (Lanoszka 2019). In addition, the Baltic states have **integrated their minority populations** far better than is often assumed. Although many Russophones may still lack citizenship rights in Estonia and Latvia and so are more likely to experience political discrimination and economic hardship, they nevertheless retain key benefits associated with living in the European Union (Trimbach and O’Lear 2015). They may have sympathies for aspects of Russian foreign policy, but these sympathies **do not translate** into a preference to be **reunited with Russia** (Kallas 2016). Accordingly, Russia faces serious obstacles **replicating what it did in Crimea**. Russians living in Crimea were generally sympathetic to being part of Russkiy Mir (‘Russian World’), making them more willing to be the objects of an annexation effort (O’Loughlin, Toal, and Kolosov 2016, 761). Further, Russia does not have an **existing military presence** in the Baltic countries—as it did with the Black Sea Fleet stationed in Sevastopol—that it could leverage to achieve easy faits accomplis and dissuade potential challengers from organizing.

In sum, NATO does not need to have a heavy footprint in the Baltic region to **deter Russian aggression**. Russia would have to overcome major operational challenges if it wished to undertake a successful conquest of the Baltic countries. Of course, none of this is to invite complacency about Baltic security. The Baltic states and Poland should deepen regional cooperation in order to ensure that no key policy differences exist between them (Jermalavicius et al. 2018). They also face potential vulnerabilities at sea and so need to improve the resilience of their undersea and maritime infrastructure (Schaub et al. 2017). Still, the **defensibility** of the Baltic region helps illuminate why Russia **resorts to disinformation campaigns**, airspace incursions, vague nuclear threats, and other attempts at subversion. It **cannot do much more** lest it would **provoke an unwanted response**.

**Russia won’t and cant expand hybrid attacks**

Dr. Samuel **Charap 16**, Ph.D. in Political Science from the University of Oxford, M.Phil. in Russian and East European Studies from the University of Oxford, B.A. in Political Science and Russian from Amherst College, Senior Fellow for Russia and Eurasia at the International Institute for Strategic Studies, “The Ghost of Hybrid War”, Survival, Volume 57, Number 6, December 2015 – January 2016

Secondly, the **setting** of eastern Ukraine made Moscow’s objective **far easier** to pursue. In fact, the region is the **most permissive environment** outside Russia’s borders for this kind of operation. The Donbas shares with Russia a **common language**, as well as **historical and cultural traditions**. It is connected to Russia by **thick cross-border interpersonal ties**. Russian business and **intel**ligence networks deeply penetrate the region. The Russian military had **near-complete** knowledge of the battlefield, and, given the highly porous border, thousands of kilometres of access to the theatre. Ukraine’s already weak governance had essentially collapsed in the east after the revolution. And there was already widespread resentment among the population towards the post-Maidan government. Polling data from April 2014 showed that over 70% of residents of the Donetsk and Luhansk regions considered the new government in Kiev ‘illegal’.11 In short, eastern Ukraine is perhaps **the only place beyond Russia’s borders where Moscow can sustain an insurgency**, and events in early 2014 made it an even softer target. As a counterfactual, one could imagine the fate of a hypothetical deployment of **‘little green men’** to Lvov, the traditional home of Ukrainian nationalism located in the west of the country. They would likely have **end**ed up **hanging from the lamp posts**, not leading an armed insurgency.

### 1NC --- Democracy D

#### Democracy resilient but doesn’t solve

Doorenspleet 18 --- Renske Doorenspleet, associate professor at the Department of Politics and International Studies, Warwick University, in the United Kingdom, Chapter 7: CONCLUSION: RETHINKING THE VALUE OF DEMOCRACY”, First Online: 22 July 2018, Page 239-243, https://link.springer.com/chapter/10.1007/978-3-319-91656-9\_7

The value of democracy has been taken for granted until recently, but this assumption seems to be under threat now more than ever before. As was explained in Chapter 1, democracy’s claim to be valuable does not rest on just one particular merit, and scholars tend to distinguish three different types of values (Sen 1999). This book focused on the instrumental value of democracy (and hence not on the intrinsic and constructive value), and investigated the value of democracy for peace (Chapters 3 and 4), control of corruption (Chapter 5) and economic development (Chapter 6). This study was based on a search of an enormous academic database5 for certain keywords,6 then pruned the thousands of articles down to a few hundred articles (see Appendix) which statistically analysed the connection between the democracy and the four expected outcomes.

The first finding is that a reverse wave away from democracy has not happened (see Chapter 2). Not yet, at least. Democracy is not doing worse than before, at least not in comparative perspective. While it is true that there is a dramatic decline in democracy in some countries,7 a general trend downwards cannot yet be detected. It would be better to talk about ‘stagnation’, as not many dictatorships have democratized recently, while democracies have not yet collapsed.

Another finding is that the instrumental value of democracy is very questionable. The field has been deeply polarized between researchers who endorse a link between democracy and positive outcomes, and those who reject this optimistic idea and instead emphasize the negative effects of democracy. There has been ‘no consensus’ in the quantitative literature on whether democracy has instrumental value which leads some beneficial general outcomes. Some scholars claim there is a consensus, but they only do so by ignoring a huge amount of literature which rejects their own point of view. After undertaking a large-scale analysis of carefully selected articles published on the topic (see Appendix), this book can conclude that the connections between democracy and expected benefits are not as strong as they seem. Hence, we should not overstate the links between the phenomena.

The overall evidence is weak. Take the expected impact of democracy on peace for example. As Chapter 3 showed, the study of democracy and interstate war has been a flourishing theme in political science, particularly since the 1970s. However, there are four reasons why democracy does not cause peace between countries, and why the empirical support for the popular idea of democratic peace is quite weak. Most statistical studies have not found a strong correlation between democracy and interstate war at the dyadic level. They show that there are other—more powerful—explanations for war and peace, and even that the impact of democracy is a spurious one (caveat 1). Moreover, the theoretical foundation of the democratic peace hypothesis is weak, and the causal mechanisms are unclear (caveat 2). In addition, democracies are not necessarily more peaceful in general, and the evidence for the democratic peace hypothesis at the monadic level is inconclusive (caveat 3). Finally, the process of democratization is dangerous. Living in a democratizing country means living in a less peaceful country (caveat 4). With regard to peace between countries, we cannot defend the idea that democracy has instrumental value.

Can the (instrumental) value of democracy be found in the prevention of civil war? Or is the evidence for the opposite idea more convincing, and does democracy have a ‘dark side’ which makes civil war more likely? The findings are confusing, which is exacerbated by the fact that different aspects of civil war (prevalence, onset, duration and severity) are mixed up in some civil war studies. Moreover, defining civil war is a delicate, politically sensitive issue. Determining whether there is a civil war in a particular country is incredibly difficult, while measurements suffer from many weaknesses (caveat 1). Moreover, there is no linear link: civil wars are just as unlikely in democracies as in dictatorships (caveat 2). Civil war is most likely in times of political change. Democratization is a very unpredictable, dangerous process, increasing the chance of civil war significantly. Hybrid systems are at risk as well: the chance of civil war is much higher compared to other political systems (caveat 3). More specifically, both the strength and type of political institutions matter when explaining civil war. However, the type of political system (e.g. democracy or dictatorship) is not the decisive factor at all (caveat 4). Finally, democracy has only limited explanatory power (caveat 5). Economic factors are far more significant than political factors (such as having a democratic system) when explaining the onset, duration and severity of civil war. To prevent civil war, it would make more sense to make poorer countries richer, instead of promoting democracy. Helping countries to democratize would even be a very dangerous idea, as countries with changing levels of democracy are most vulnerable, making civil wars most likely. It is true that there is evidence that the chance of civil war decreases when the extent of democracy increases considerably. The problem however is that most countries do not go through big political changes but through small changes instead; those small steps—away or towards more democracy—are dangerous. Not only is the onset of civil war likely under such circumstances, but civil wars also tend to be longer, and the conflict is more cruel leading to more victims, destruction and killings (see Chapter 4).

A more encouraging story can be told around the value for democracy to control corruption in a country (see Chapter 5). Fighting corruption has been high on the agenda of international organizations such as the World Bank and the IMF. Moreover, the theme of corruption has been studied thoroughly in many different academic disciplines—mainly in economics, but also in sociology, political science and law. Democracy has often been suggested as one of the remedies when fighting against high levels of continuous corruption. So far, the statistical evidence has strongly supported this idea. As Chapter 5 showed, dozens of studies with broad quantitative, cross-national and comparative research have found statistically significant associations between (less) democracy and (more) corruption. However, there are vast problems around conceptualization (caveat 1) and measurement (caveat 2) of ‘corruption’. Another caveat is that democratizing countries are the poorest performers with regard to controlling corruption (caveat 3). Moreover, it is not democracy in general, but particular political institutions which have an impact on the control of corruption; and a free press also helps a lot in order to limit corruptive practices in a country (caveat 4). In addition, democracies seem to be less affected by corruption than dictatorships, but at the same time, there is clear evidence that economic factors have more explanatory power (caveat 5). In conclusion, more democracy means less corruption, but we need to be modest (as other factors matter more) and cautious (as there are many caveats).

The perceived impact of democracy on development has been highly contested as well (see Chapter 6). Some scholars argue that democratic systems have a positive impact, while others argue that high levels of democracy actually reduce the levels of economic growth and development. Particularly since the 1990s, statistical studies have focused on this debate, and the empirical evidence is clear: there is no direct impact of democracy on development. Hence, both approaches cannot be supported (see caveat 1). The indirect impact via other factors is also questionable (caveat 2). Moreover, there is too much variation in levels of economic growth and development among the dictatorial systems, and there are huge regional differences (caveat 3). Adopting a one-size-fits all approach would not be wise at all. In addition, in order to increase development, it would be better to focus on alternative factors such as improving institutional quality and good governance (caveat 4). There is not sufficient evidence to state that democracy has instrumental value, at least not with regard to economic growth. However, future research needs to include broader concepts and measurements of development in their models, as so far studies have mainly focused on explaining cross-national differences in growth of GDP (caveat 5).

Overall, the instrumental value of democracy is—at best—tentative, or—if being less mild—simply non-existent. Democracy is not necessarily better than any alternative form of government. With regard to many of the expected benefits—such as less war, less corruption and more economic development—democracy does deliver, but so do nondemocratic systems. High or low levels of democracy do not make a distinctive difference. Mid-range democracy levels do matter though. Hybrid systems can be associated with many negative outcomes, while this is also the case for democratizing countries. Moreover, other explanations—typically certain favorable economic factors in a country—are much more powerful to explain the expected benefits, at least compared to the single fact that a country is a democracy or not. The impact of democracy fades away in the powerful shadows of the economic factors.8

### Ext --- Democracy D

#### Alt causes

Klaas ’21 [Brian; June 11; associate professor of global politics at University College London; the Washington Post, “Opinion: The world is horrified by the dysfunction of American democracy,” https://www.washingtonpost.com/opinions/2021/06/11/pew-research-global-opinion-us-democracy/]

It’s official: America is no longer a “shining city upon a hill.”

Data released Thursday from Pew Research shows that our allies are beyond delighted that the Trump presidency has ended. Confidence in U.S. leadership has soared. Our friends are breathing a sigh of relief.

But buried in that story about the United States’ post-Trump redemption is some seriously bad news: U.S. allies see our democracy as a shattered, washed-up has-been. We used to provide a democratic model for the world, but no longer. The chaos, dysfunction and insanity of the past several years have taken a predictable toll.

The numbers are depressing. Just 14 percent of Germans see American democracy as a desirable model for other countries, while 54 percent say that it “used to be a good example, but has not been in recent years.” Public opinion in France, Britain, South Korea, Japan and Australia is similarly bleak. In New Zealand, fewer than 1 in 10 citizens sees American democracy as a desirable model.

It turns out the rest of the democratic world wasn’t particularly impressed by the United States’ former authoritarian president, who spread conspiracy theories, tweeted narcissistic absurdities while 400,000 people died of covid-19, and incited a deadly insurrection. Go figure.

But these numbers coming out of our allies aren’t just depressing bits of polling trivia. They have real-world consequences. And they highlight a disturbing, inescapable dilemma that the Biden administration must confront: Until the United States fixes its broken democracy at home, it will be unable to effectively fight authoritarianism abroad.

Put bluntly: The United States’ authoritarian slide isn’t just a domestic policy issue. It’s a foreign policy disaster, too.

Ever since Donald Trump emerged as the Republican front-runner in 2016, China has been exploiting the unhinged turmoil he ushered in as evidence that democracy is a bad joke rather than a serious way of governing a society. As the Trump years descended into mayhem, China ramped up its rhetoric. And when Trump’s failures to contain the covid-19 pandemic became plain for the world to see, Beijing cited it as further evidence that democracy was a failed experiment.

Needless to say, China is no model for the rest of the world; it’s a brutal authoritarian regime that stays in power by committing genocide against ethnic and religious minorities while silencing its critics. But the Trump years were a gift-wrapped propaganda coup for the Chinese in their ongoing battle to challenge the West’s ideological primacy on the global stage.

This matters because emerging economies are slowly getting pulled into China’s orbit as they seek a viable blueprint for their own development. In Afrobarometer surveys of public opinion across Africa, China has pulled even with the United States. Six in 10 Africans have a favorable view of China’s role in their country. And while the United States is still seen as offering the best development model, China isn’t far behind. This is a drastic shift in just a few decades — and it will play an increasingly important role in U.S. foreign policy as some of these developing countries decide whether to follow Washington or Beijing.

The United States has lost the moral high ground. The world might have always been wary of lectures from the United States about the virtues of democracy and freedom, but at least those on the receiving end of those lectures often believed that the country giving the lecture knew how to build a successful democracy. That’s no longer true.

At a time of authoritarian resurgence, we need the words of the U.S. president to pack a democratic punch. Instead, they ring hollow. After all, due to ongoing Republican machinations, American voters can’t even be sure that their right to vote will be protected in the years to come. What can the United States teach the world about democracy when the country is continuing its steady slide toward authoritarian politics?

This won’t just hamper President Biden’s foreign policy; it will also make the world safer for authoritarianism. Although there are still plenty of desirable democratic models around the world (I’m looking at you, Norway), none of them has the power to take meaningful action when a dictator rigs an election or imprisons an opposition leader. Worse, now that the world doesn’t respect or admire U.S. democracy, dictators have a rhetorical trump card. They can point to the fact that Trump (falsely) claimed the U.S. election was rigged; that Republicans are actually trying to rig elections with voter suppression and worsened partisan gerrymandering; and that the former president repeatedly called to jail his political opponents. Our hypocrisy will enhance dictators’ impunity.

Comparisons between the United States’ malfunctioning politics and genuine dictatorships are, of course, hyperbolic. But dictators will nonetheless get plenty of rhetorical mileage out of making them, pointing to Washington’s failures to justify or excuse their own authoritarian plots.

#### Democratic peace theory is cherry-picked, and dyadic between two democracies at best.

Doorenspleet ’19 [Renske; 2019; Political Science and International Studies Professor at Warwick University; Rethinking the Value of Democracy: A Comparative Perspective, “Democracy and Interstate War,” Ch. 3]

This finding or ‘law’ has not only been recognized by scholars of international relations, but also found its way outside academia and has influenced foreign policies to promote peace and democracy, most prominently since the 1990s. However, my book will not draw conclusions based on ‘cherry-picking’ of specific studies showing how peaceful democracies are, but on a systematic overview of studies in this field. Therefore, this book relies on my own database with hundreds of different studies, which are relevant for each chapter; the articles had to engage directly with the chapter’s main research question. The next section will provide more detailed information around the selection criteria. This overview includes both highly cited and recent articles which were selected in a systematic way.

Based on analyses of statistical studies around this topic of democracy and war, it will become clear that the overall statistical support for the democratic peace hypothesis is not strong at all. In the rest of the chapter, I will spell out four reasons why democracy does not cause peace, and why the empirical support for the popular idea of democratic peace is quite weak: (1) most studies do not find a strong correlation between democracy and interstate war at the dyadic level, and they show that there are other—more powerful—explanations for war and peace, or even that the impact of democracy is a spurious one, (2) the theoretical foundation of the democratic peace hypothesis is weak, and the causal mechanisms are unclear, (3) democracies are not necessarily more peaceful in general, and the evidence for the democratic peace hypothesis at the monadic level is inconclusive, and (4) the process of democratization is dangerous and living in a democratizing country means living in a less peaceful country.

In my view, it is difficult—if not impossible—to support the democratic peace hypothesis without any reservations. The key caveats should not be ignored and certainly deserve more attention before we can confidently argue that democracies are more peaceful than other types of political systems. Please notice that I can already reveal that the assumed link between democracy and intrastate war is problematic as well, but this topic will be at the core of the next chapter (Chapter 4).

Selection of Articles: Democracy and War

The instrumental value of democracy cannot convincingly be found in democracy’s expected bond with peace. I have come to this conclusion on the basis of an analysis of statistical studies, which will be discussed in the rest of this chapter. So how did I select the articles for my database?4

For this chapter and Chapter 4, I selected the articles that focused on war and democracy. Using the online database Web of Science (formerly known as Web of Knowledge), I identified a total of almost 8000 articles published in the sampled journals until the end of 2015. I identifed them by entering ‘democr\*’ in the basic search field; this asterisk (\*)-based ‘wildcard’ allows searching for terms including ‘democratic’, ‘democracy’, and ‘democratization’ (in both British and American spellings) simultaneously, in the title, abstract and/or the keywords. As a next step, I excluded articles in which ‘democracy’ is used as synonym for state (e.g. analysis of the relationship between immigration policies and unemployment in European democracies) or a specific political party or movement (e.g. the ‘Democrats’ in the USA, or Uganda’s People’s Democratic Army) or a specifc country (e.g. the Democratic Republic of Congo). In addition, I identified them by entering ‘war\*’ in the basic search feld. The words democracy (democr\*) and war (war\*) need to be mentioned in title and/or abstract—and I also checked for equivalents of ‘war’ like ‘conflict’ and ‘dispute’ and ‘no peace’.5

As it is not feasible to analyse thousands of articles, it is necessary to take a next step in the selection process. I decided to select these articles, which will be part of the database for the third and fourth chapter, in three different ways. The first method is to choose the articles with the most citations. So, for example, in Chapter 3, the articles which are cited more than a hundred times are included in this first list. The article by Beck et al. (1998) has been cited more than 951 times, and as a consequence, this article is part of the database. But also articles with a much lower number of citations (such as Barbieri 1996, with 179 citations) are included in my analyses.

The second method is simply to include the most recent articles published in the past five years, so since beginning 2011 until end 2015. The most recent articles can easily be overlooked by applying the first method of most quoted articles. In my view, however, they still need to be included as they present the most recent findings and engage with the recent and innovative debates, which cannot be ignored in this book. For example, recent studies on democracy and interstate war (Chapter 3) have paid more attention to the mechanisms (see, e.g., Zeigler et al. 2014), and there is a growing attention for the impact of political institutions in recent studies on democracy and intrastate war (Chapter 4; see, e.g., Walter 2015). Those recent findings cannot be ignored in any systematic analysis of statistical studies on this theme.

The third method is the most subjective approach of selecting articles, as it is based on the ‘snowballing method’. So it includes articles which have not been selected by the first and second methods, but which have been quoted extensively and regularly by the previously selected articles. For example, the article by Bethany Lacina (2006) cannot be selected based on having high citations (the first method) and it cannot be included based on being a recent publication (the second method), but it has been mentioned by key studies and hence surfaces via the snowballing method (a third method). This article is important as it clearly distinguishes the determinants of conflict severity from those for conflict onset, and those determinants seem to be quite different, which is crucial information for Chapter 4.

In this way, my study presents and assesses the findings based on a big pool of statistical studies in the published literature. Based on this assessment, I will be able to draw clearer conclusions concerning the significance of the effects of democracy on interstate war (this chapter) and intrastate war (the next chapter). The Appendix shows more detailed information of the selected articles.

The Democratic Peace Hypothesis, Its Roots and Supporters

The democratic peace hypothesis6 states that democracies never or seldom go to war with one another. Where is this powerful idea of ‘democratic peace’ coming from? Before discussing the main findings of the statistical articles and before describing the four caveats of the ‘democratic peace paradigm’, we need to know a bit more around the background and the roots of this idea.

Immanuel Kant’s 1795 essay Perpetual Peace has often been mentioned as the foundation for this hypothesis. Kant believed peace was difficult to achieve, since ‘the natural state is one of war’ (Kant 1795: 10). A state of peace must therefore be established for—in his view—it is certain that hostilities will be committed and people need to be protected from each other. In such a world, each may treat his neighbour, from whom he demands security, as an enemy. In a dictatorship where ‘the subjects are not citizens, a declaration of war is the easiest thing in the world to decide upon, because war does not require of the ruler, who is the proprietor and not a member of the state, the least sacrifice of the pleasures of his table, the chase, his country houses, his court functions, and the like. He may, therefore, resolve on war as on a pleasure party for the most trivial reasons, and with perfect indifference leave the justification which decency requires to the diplomatic corps who are ever ready to provide it’ (Kant 1795: 13).

In contrast, the situation is different in constitutional republics, according to Kant. He argued that the majority of the people in republics would never vote to go to war, except for pure self-defence. Therefore, a world with only republics would be peaceful, since there would be no aggressors. The republican constitution, which requires the consent of the citizens to start a war, gives the positive prospect of perpetual peace.

It is important to note that the ideas of Kant on the one hand and the modern democratic peace scholars on the other hand are not completely similar. For example, Kant talked about republics instead of democratic states as the ideal states to achieve peace. He defined republican states as states with representative governments, in which the legislature is separated from the executive. Not surprisingly—considering the epoch in which he lived—Kant did not include universal suffrage in his definition, which is now seen as an essential dimension of democracy, even of the most minimalist types of democracy (Dahl 1971; see also Chapter 2). Moreover, Kant argued that republics will be at peace in general, which means that such political systems are expected to be not only in peace with each other, but also with other non-republican systems. Nowadays, only few scholars would support this approach of a ‘monadic democratic peace’. As will become clear at the end of this chapter, there is not much evidence for the idea that democracies are more peaceful in general.

Since the 1960s, most statistical studies have not focused on the ‘monadic democratic peace hypothesis’ but on testing the ‘dyadic democratic peace hypothesis’. This dyadic hypothesis states that it is less likely that democracies fight with each other, compared to other ‘dyads’ or other pairs of different types of political systems. The sociologist Dean Babst was the first scholar who started to build on Kant’s old idea in the ‘dyadic’ way, and decided to test it in statistical studies (Babst 1964, 1972). He concluded that ‘no wars have been fought between independent nations with elective governments between 1789 and 1941’ (Babst 1972: 55). His study was not published in one of the journals in the field of international relations, but in a sociological journal and later in Industrial Research. Therefore, it was not read by international relations scholars, and initially, it did not get the attention it deserved in the field of international politics.

Babst’s work was, for example, not cited by Melvin Small and J. David Singer (1976), and their fndings seemed to contradict Babst’s study. However, Small and Singer did not compare the rates of war proneness for democracies and dictatorships, but instead they focused on the question whether wars involving democratic states have historically been significantly different in length or in degree of violence compared to wars involving only dictatorships. For length and degree of violence during the wars, they did not find a difference between democracies and dictatorships, so they concluded that types of political systems did not matter.7 A few years later, Rudolph J. Rummel did cite Babst’s work and replicated Babst’s idea in statistical tests, which were described in the fourth book of his five-volume Understanding Confict and War (1975– 1981). He found clear support for his eleventh (of the 33) propositions about causes and conditions of conflict, which stated that ‘Libertarian systems mutually preclude violence’ (Rummel 1979: 279).

Eventually, those innovative studies from the 1970s helped to evoke the interest in the democratic peace proposition, and in the expected peaceful nature of relationships among democratic states. Since the 1980s, the number of quantitative studies has increased considerably, accumulating into an impressive field of research in international relations with its own ‘empirical law’ of democratic peace (Levy 1989: 270; see also Ray 1998).

This democratic peace hypothesis has not only received support from political scientists, but also from politicians and policy makers. Particularly since 1993, the idea of a democratic peace has inspired American foreign policies aimed at the promotion of peace and democracy. As the 42nd president of the USA (1993–2001), Bill Clinton was the first politician who explicitly bridged the gap between these findings in international relations on the one hand, and his foreign policy strategy on the other hand, at least rhetorically. Anthony Lake, who was Clinton’s National Security Adviser, stated in 1993 that in order to cope with America’s foreign policy challenges, the expansion of democratic states around the world would be essential because ‘it protects our [U.S.] interests and security’ (see Henderson 2002: 20). In his 1994 State of the Union, Clinton declared that ‘Ultimately, the best strategy to ensure our security and to build a durable peace is to support the advance of democracy elsewhere. Democracies don’t attack each other’.8 Findings from research in the field of international relations seemed to have a direct impact on policy making, and this move of the Clinton administration can be seen as ‘a textbook case of arbitrage between the ivory tower and the real world’ (Gowa 1999: 109).

Clinton’s successor, George W. Bush, went one big step further in his faith that democratic peace holds. He argued that efforts to turn Iraq into a democratic country would have positive effects on Iraqi’s neighbours. The authoritarian regimes in the region would fall as domino stones and follow the Iraqi example. They would start democratizing as soon as they could, which would then result in achieving a peaceful and stable the Middle East. The real motives for attacking Iraq may have been different, but ‘regime change’ was at the heart of Washington’s rhetoric when the USA started to bomb Baghdad in March 2003. The rhetoric of the Bush administration focused on toppling Saddam Hussein’s regime, and replacing the entire underlying dictatorial system with a democracy.

Moreover, George W. Bush used the democratic peace idea to justify the war in Iraq, declaring, ‘The reason why I’m so strong on democracy is democracies don’t go to war with each other…I’ve got great faith in democracies to promote peace. And that’s why I’m such a strong believer that the way forward in the Middle East, the broader Middle East, is to promote democracy’.9 In 2004, the 43rd President of the USA said: ‘If you think you can have peace without democracy – again - I think you’ll find that - I can only speak for myself, that I will be extremely doubtful that it will ever happen’.10 In his second inaugural address, he stated that ‘the survival of liberty in our land increasingly depends on the success of liberty in other lands. The best hope for peace in our world is the expansion of freedom in all the world’.

Again, these are just words from speeches and can hence be seen as rhetoric to defend military intervention (cf. Jervis 2003; Kaufmann 2004; Daalder and Lindsay 2005; Owen 2005; Lieberfeld 2005; Schmidt and Williams 2008). Still, in the end, politicians have rationalized their political decisions based on one of the most powerful ideas taken from studies in the field of international relations, clearly showing the influence of this academic idea in political practice.

Hence, the field of international relations seems to have its own law: democracies rarely fight with each other. It cannot be denied that the evidence supporting the democratic peace proposition is quite diverse in character (see Ray 1998): the evidence has been epistemological (Rummel 1975), philosophical (Doyle 1986), formal (Bueno de Mesquita and Lalman 1992), historical (Weart 1994; Ray 1995; Owen 1994), experimental (Mintz and Geva 1993), anthropological (Ember et al. 1992; Crawford 1994), psychological (Kegley and Hermann 1995), economic (Brawley 1993; Weede 1996) and political (Gaubatz 1991). Still, there have been numerous critical studies (see, i.e., Hayes 2011), and the general picture is unclear. We do not yet know much about the overall findings from statistical studies.

So far, it seems as if some quantitative studies—mainly within the field of international relations—have found strong and robust evidence which supports the ‘democratic peace hypothesis’. Those studies show that democracy has had a positive influence on international peace (see, i.e., Rummel 1979; Ray and Russett 1996). In this sense, the idea of a democratic peace seems to be confirmed. Political scientists such as James Lee Ray are passionate supporters: ‘No scientific evidence is entirely definitive’ but ‘based on all the empirical evidence so far’ the more defensible of the two possible definitive answers to the question “Does democracy cause peace?” is “Yes” (Ray 1998: 43). However, based on my own analyses of the empirical studies with statistical evidence, I cannot be as enthusiastic as those scholars; to the contrary, I whole-heartily disagree with them, as a more systematic analysis of the articles shows that there are four important weaknesses, which seriously undermines the idea that peace is one of democracy’s instrumental values.

Caveat 1: It’s Not (Just) Democracy

While analysing the selected articles, the first remarkable finding is that only a relatively small number of studies have actually tested the democratic peace hypothesis. Most of the studies have focused on the mechanisms (see next section, caveat 2), and hence seem to assume that there is a correlation between democracy and war. In this way, the majority of the studies—often unintentionally—reinforce the idea that democratic peace actually exists without testing this proposition. However, none of the studies that directly test the democratic peace hypothesis found strong evidence that democracy is the most important factor when explaining interstate war. All democratic peace studies have controlled for many possible alternative causes of the peace, such as economic development and growth, geographic distance and contiguity, power status, alliance ties, militarization and political stability. The findings show that it is not just democracy which explains war, not at all. Within this group of studies, which explicitly test the democratic peace hypothesis, four different types of findings can be detected. I will discuss those results more in-depth in the rest of this section.

First Result: There Is Correlation, but Other Explanations Are Significant Too

The first subgroup consists of scholars who stress the importance of democratic peace, despite the fact their own analyses have shown that other factors are statistically significant as well (Maoz and Russett 1993; Rousseau et al. 1996; Gleditsch and Hegre 1997; Beck et al. 1998; Ray 2013). For example, some studies (e.g. Rousseau et al. 1996) included alternative independent variables in order to test realist arguments. They tested whether the distribution of power determines decisions to use force, and measures each state’s military capabilities relative to its opponent. A state’s military capability is the average of three elements: number of troops, military expenditures and military expenditures per soldier. They found that this realist variable was strong, positive and statistically significant at the 0.001 level in their analyses (see, e.g., Rousseau et al. 1996: 522, Table 2). However, not only a state’s military capabilities appeared to be an important explanation for peace. In addition, wealth, growth, alliances and contiguity played a crucial role when explaining interstate war (see, e.g., Maoz and Russett 1993: 632, Table 1).11 Moreover, when other factors are included, the impact of democracy on the likelihood of international crises is even spurious (Maoz and Russett 1993: 632; Henderson 2002: 141, see also p. 3).12 Still, scholars in this group keep defending the democratic peace idea, despite the fact that their own analyses showed the significance of alternative explanations.

Second Result: Initially There Is Correlation, but the Impact of Democracy Is Spurious When Other Explanatory Factors Are Included in the Models

The second subgroup of scholars is far more radical. Based on their own analyses, this group concludes that the democratic peace link is a spurious one (Weede 1984, 1996; Barbieri 1996; Mousseau 2013; Gartzke and Weisiger 2014).13 Typically, efforts to demonstrate the spuriousness of the statistical democratic peace pointed to other factors that, when accounted for ‘properly’, eliminated or dramatically reduced the statistical significance of shared democracy. Hence, the studies in this second group did not find strong evidence for the democratic peace hypothesis anymore, once other explanatory factors were included in the models.14

One of the most convincing alternative explanations of peace between countries is that there is no democratic peace, but a capitalist peace instead. The settlement in Germany and Japan succeeded because of the establishment of capitalist peace. Because of economic support by the Americans, who encouraged free trade and offered trade opportunities in practice as well, the poorer economies in Europe and Japan would gain economically, resulting in ‘economic growth, prosperity, and, ultimately, free trade among most of the more technologically advanced economies’ (Rasler and Thompson 2005: 232). By establishing and expanding free trade, the incentives for war would quickly decrease among trading states, according to this approach. To prevent new interstate wars after World War II, the capitalist peace was a far more important factor than the American promotion of democracy and its political institutions.

The capitalist peace, or capitalist peace theory, also states that economic development accounts for both democracy and the peace among democratic nations. Economic development is a key factor to explain democracy (Lipset 1959; see also Hegre 2003; Weede 2004).15 Moreover, economic development also plays a role when explaining peace, and the presence of market-oriented economies in countries have a positive impact on both democracy in those countries and peace between them (Mousseau 2000, 2002, 2003, 2005, 2013; see also Hegre 2014). Democratic peace only exists when both democracies have high levels of economic development, when economic development is well above the global median.

In fact, the poorest 21% of the democracies studied, and the poorest 4–5% of current democracies, are significantly more likely than other kinds of political systems to fight each other (see, e.g., Mousseau 2005). Moreover, if at least one of the democracies involved has a very low level of economic development, then democracy cannot prevent war.16 Still, there is a pacifying effect of free trade and economic interdependence, which is more important than the effect of democracy, because the former affects peace both directly and indirectly, by producing economic development and ultimately, democracy (see Weede 2004).17

Capitalist peace is not the only alternative explanation. Shared interests in general, and political similarities in specific, can also be seen as an important second alternative explanation for war and peace between countries (Farber and Gowa 1995, 1997; Gartzke 2007; Gowa 1999; Henderson 2002). Democracies are not peaceful to each other because they are democratic, but rather because they are similar. So the difference of the scores of both countries also contributes to the conflict proneness of the dyad. If the difference in levels of democracy is big, then the chance of conflict is higher (cf. Oneal and Russett 1997: 281–282).

Many researchers have conflated both the conflict-dampening impact of joined democracy and the confict-exacerbating impact of political distance in the variables focusing on political systems, but as Errol A. Henderson (2002: 32) convincingly argued: ‘Fusing these two contrasting attributes in a single variable makes it difficult to distinguish between the competing processes’. Therefore, it is better to include an additional variable of ‘political dissimilarity’ in the model. Henderson (2002) was one of the first scholars who included this variable and measured it by taking the absolute value of the difference between the two states’ scores. His main variables were not only political similarity, but also geographic distance and economic interdependence, and he concluded that democratic peace is a statistical artefact which disappears when those other variables are taken into account. Political similarity clearly has a pacifying effect18 (see Werner 2000; Henderson 2002; Beck et al. 2004), and it is not democracy per se which is the decisive factor.19

Hence, the benefits of trade and trade interdependence are essential explanations, while democracy is spurious or at least subordinate (see also Rosecrance 1986; Weede 1984, 1996; Hegre 2000, 2014; Jervis 2002; Souva 2003; Rasler and Thompson 2005: 235; Mousseau 2000, 2002, 2003, 2005). Based on those studies, it is safe to conclude that democracy, on its own, is an unlikely cause of the democratic peace.

Third Result: There Is Correlation, but Other Explanations Are Much Stronger

This same point that democracy is just one of the explanations for peace (and not even a very important one) is also at the core of studies in the third subgroup. Scholars of this group keep arguing that there is support for the democratic peace hypothesis, and that the link is not spurious. In this sense, they are less radical than the second group of scholars, as they do not completely reject the value of democracy for peace. On the other hand, their own analyses have clearly shown that alternative factors—hence other factors than democracy or type of political system— are not only statistically significant but also more important when trying to explain interstate war (Bremer 1992; Gelpi 1997; Oneal and Russett 1999a, b; Reiter and Stam 2002; Peterson 2013; Caselli et al. 2015).

Theoretical arguments and empirical evidence suggest that democracy is not the most important factor, while war is more likely to occur between states that are geographically proximate, approximately equal in power, major powers, allied, economically advanced and highly militarized than between those that are not. Bivariate analyses of these factors in relation to the onset of interstate war over all pairs of states in the period from 1816 to 1965 have generally supported these associations. However, multivariate analyses revealed some differences. Stuart Bremer (1992), for example, showed that some factors are far more important than others. The existence of a dangerous, war-prone dyad can be best explained by the presence of contiguity, the absence of an alliance and the absence of more advanced economy. The absence of democratic polity and other factors (absence of overwhelming preponderance, and presence of major power) are less powerful. Overall, these findings suggest that our research priorities may be seriously distorted and that we should not focus too much on the perceived positive impact of democracy, but on other factors (such as alliances and economic factors) instead.

Fourth Result: There Is Correlation, but Only Under Certain Specific Conditions

The final subgroup of scholars argues that we cannot unconditionally accept the idea that democratic peace exists in general, so always and everywhere. Their statistical studies clearly showed that support for this hypothesis heavily depends on other factors. The chance of democratic peace depends not just on the specific historical period (Cold War or not; Gibler and Sarkees 2004; Siverson and Emmons 1991; Weede 1984), but also the stage of the conflict (beginning, duration or severity; see Bremer 1993; Bennett and Stam 1996; Reed 2000), and on the neighbourhood instability (extent of confict in the region; see Gibler and Braithwaite 2013; Gibler and Miller 2013). Despite the differences between the studies, there is one common finding in all studies: when explaining interstate war, we cannot just rely on the impact of democracy, as it is too much dependent on other factors.

Several scholars found strong evidence for the idea that democratic peace exists, but only during some specific historical periods. Based on this evidence, they concluded that democratic peace is simply a statistical artefact of the Cold War. For example, Henry Farber and Joanne Gowa (1995) found statistical support for the idea that peace between democracies is an artefact of the Cold War, when the threat from the communist states forced democracies to ally with one another (see also Mearsheimer 1990). Sebastian Rosato (2003) also argued that most of the significant evidence for democratic peace has been observed after World War II; and that it has happened within a broad alliance, which can be identified with NATO and its satellite nations, imposed and maintained by American dominance.

Since the Second World War, war has become a very costly affair. Scholars discovered that only a handful of states are ‘capable of engaging in major power warfare. That process of elimination has not yet extinguished the possibility of major power warfare, but it has lowered its probability immensely’ (Rasler and Thompson 2005: 219). The chance to achieve something in a war is low in general, and even lower in a bipolar world with two big power players risking high nuclear war costs (Jervis 2002). While war became more costly, trade became less costly; as a consequence, the war/trade costs increased during the Cold War (Rosecrance 1986; see also Jervis 2002). In such a world, war and conflict have become less attractive, while trade and cooperation have become more appealing (Rasler and Thompson 2005: 219). Hence, more states decided to adopt trading strategies in order to prevent confict and war as much as possible. In the end, democracy was part of the story, but only a very small part with a subordinated role next to the power dynamics during the Cold War, the costs of warfare and the benefits of trade.

Some scholars found evidence that the democratic peace still exists in the post-Cold War period (Park 2013) which weakens this argument. However, most analyses showed that dyadic dispute rates have converged after the Cold War (see, e.g., Gowa 2011). Moreover, jointly democratic dyads are likely to be allied only after 1945 (see Gibler and Sarkees 2004); during the 1816–1944 time period, there is even a negative relationship between democratic dyads and alliance formation.20 These findings cast serious doubts on the idea of a general existence of democratic peace.

Not only the historical period, but also the *stage* of the conflict is crucial. Some scholars in this group provided evidence that democratic peace is not universal, but that it depends on the stage and whether we focus on the beginning, duration or severity of the conflict. Although joint democracy has some pacifying effects on the onset of conflict, the results suggest that they are unrelated to the escalation of disputes to war (see Reed 2000). Moreover, democratic peace is dependent on the neighbourhood instability. Democracies often have few territorial issues over which to contend, as they tend to be part of a stable region. Democracies only seldom have territorial disputes with their neighbours, and therefore they can more easily choose favourable conflicts to escalate. The type of political system does not predict conflict selection or victory once controls are added for issue salience (Gibler and Miller 2013; see also Park and James 2015). There is an interaction between joint democracy and regional instability, which confirms the idea that the effects of type of political system on continued conflict apply mostly to dyads in peaceful regions (Gibler and Braithwaite 2013; see also Park and James 2015). Very democratic countries might even become more aggressive and faster than other political systems, once the region becomes more hostile (see, e.g., Baliga et al. 2011).

The General Lesson from the Results in a Nutshell (Caveat 1)

In short, regardless of the differences between the statistical studies on democratic peace, all findings have indicated that other explanations are important as well. It is clear that democracy is just one of the explanations, and certainly not the most important one,21 sometimes even spurious and often heavily dependent on other factors. It is not (just) democracy to be preoccupied with, when trying to prevent war between countries (Table 3.1).

Caveat 2: What Are the Causal Mechanisms?

Most of the statistical studies on democratic peace seem to assume that there is a correlation between democracy and war; based on this assumption, they then decide to focus on the mechanisms. This is problematic as none of the democratic peace studies found strong evidence that democracy is the most important factor when explaining interstate war (see the previous section). As a consequence, the next step of looking for mechanisms is quite irrelevant and not necessary in my view, but most studies nevertheless argue that the field lacks strong theoretical foundations and robust empirical evidence that can reveal convincing causal mechanisms.22 Those studies seem to accept the correlation between dyadic democracy and peace, and then start questioning whether democracy really causes peace before investigating potential mechanisms.

Table 3.1 Statistical studies on democracy and interstate war (dyadic level)

|  |  |
| --- | --- |
| Caveat 1: It’s Not (Just) Democracy | Studies |
| ‘It’s just democracy; democracy is most important explanation for peace between countries’ | No studies found |
| ‘There is correlation, but other explanations are significant too’ | Beck et al. (1998), Gleditsch and Hegre (1997), Maoz and Russett (1993), Ray (2013), and Rousseau et al. (1996) |
| ‘Initially there is correlation, but the impact of democracy is spurious when other explanatory factors are included in the models’ | Barbieri (1996), Beck et al. (2004), Farber and Gowa (1997), Gartzke (2007), Gartzke and Weisiger (2014), Gowa (1999), Hegre (2000, 2003, 2014, Jervis (2002), Mousseau (2000, 2002, 2003, 2005, 2013), Oneal and Russett (1997), Rasler and Thompson (2005), Rosecrance (1986), Souva (2003), Weede (1984, 2004), and Werner (2000) |
| ‘There is correlation, but other explanations are much stronger’ | Bremer (1992), Caselli et al. (2015), Gelpi (1997), Oneal and Russett (1999a, b), and Peterson (2013) |
| ‘There is correlation, but only under certain specific conditions’ | Baliga et al. (2011), Bremer (1993), Bennett and Stam (1996), Farber and Gowa (1995), Gibler and Braithwaite (2013), Gibler and Miller (2013), Gibler and Sarkees (2004), Gowa (2011), Jervis (2002), Mearsheimer (1990), Park (2013), Park and James (2015), Rasler and Thompson (2005), Reed (2000), Rosato (2003), Rosecrance (1986), Gibler and Sarkees (2004), Siverson and Emmons (1991), and Weede (1984) |

#### No democratic peace

Jeff Grabmeier 15. Senior Director, Research communications, Media & PR "'Democratic peace' may not prevent international conflict". No Publication. 9-3-2015. https://phys.org/news/2015-09-democratic-peace-international-conflict.html

Using a new technique to analyze 52 years of international conflict, researchers suggest that there may be no such thing as a "democratic peace."

In addition, a model developed with this new technique was found to predict international conflict five and even ten years in the future better than any existing model.

Democratic peace is the widely held theory that democracies are less likely to go to war against each other than countries with other types of government.

In the new study, researchers found that economic trade relationships and participation in international governmental organizations play a strong role in keeping the peace among countries. But democracy? Not so much.

"That's a startling finding because the value of joint democracy in preventing war is what we thought was the closest thing to a law in international politics," said Skyler Cranmer, lead author of the study and The Carter Phillips and Sue Henry Associate Professor of Political Science at The Ohio State University.

"There's been empirical research supporting this theory for the past 50 years. Even U.S. presidents have touted the value of a democratic peace, but it doesn't seem to hold up, at least the way we looked at it."

### 1NC --- Democracy Bad

#### Democracy causes great power nuclear war –

#### 1. Security dilemma.

Muller, director of the Peace Research Institute in Frankfurt, professor of International Relations at Goethe University, 15

(Harald, Democracy, Peace, and Security, Lexington Books pp. 44-49)

My own proposal for solving the problem. developed together with my colleague Jonas Wolff (Müllcr 2004. Muller/Wolff 2006). turns the issue upside down: We do not start with explaining mutual democratic peacefulness, but its opposite. the proven capability of democracies to act aggressively against non-democracies. We note that—apart from self-defense where there is no difference between democracies and non-democracies——democratic states go to war—in contrast to non-democracies—to uphold international law (or their own interpretation thereof), to prevent anarchy through state failure, to “save strangers” when dictatorships massacre their own people, and to promote democracy. None of these acts is likely to find its target in a democracy. Since the use of force by democracies is hardly possible without public justification, even the rhetorical use of the said reasons will not stand public scrutiny when uttered against a democracy—people will not believe it, War other than for self-defense thus can only be fought by democracies against non-democracies because against a fellow democracy justification would fail. Because whether this is the case or not to a degree that justifies war as the ‘ultimate means” must rely on practical judgments. and practical judgments can differ among even reasonable people. democracies might disagree whether or not the judgment applies in specific cases. Democracies also show variance in that regard due (o a systematic. political-culturally rooted different propensity to judge situations as justifing war or not, and to participate in such wars (Gels et al, 2013). It should also be noted that, given the continuum between autocracy, anocracy and democracy, whether a given state is a democracy or not can be subject to interpretation. and this interpretation may even change over time (Oren 1995, Hayes 2013). The fact is that there are a couple of fairly warlike democracies, and that the democracies participating most frequently in military disputes (apart from the special case of Israel) are, by and large. major powers such as the United States, the United Kingdom. France. or India. This pattern is important to keep in mind when the question of the utility of democratic peace for today ‘s world problems is to be answered. Transnational terrorism, failed states, civil wars and the like dominate the international agenda on war and peace. At the classical level of international relations, in the relationships among major powers. developments arc undcr way which potentially pose an even greater threat than this diverse collection of non-interstate problems presently does. We are living in an era of rather rapid and disturbing power change (Tammcn et al. 2000). The United States are still the leading power of the world with unprecedented militany and economic poer. But others are coming closer: China. India. Braiil and Indonesia, China is at the top of this cohort, All major power changes chal lenge existing structures and thus contain the potential for great disturbance. The leading power may start to fear for its dominant position and take measures to ensure its position at the lop. These actions may frustrate emerging powers and even lead to the perception that their security is endangered. which would motivate counter-measures that further propel a political escala tion spiral. An increasingly focused competition in which a true power change appears increasingly possible. that is. a change of position at the top of the international hierarchy, has an even greater risk potential. If the inherent dangers are not contained—which remains always a possibility major power war may ensue defying all propositions that major war has become obsolete or that nuclear deterrence will prevent this calamity once and for all. Of course, states can grow peacefully into roles of higher responsibility. status and influence on the world stage. There arc no natural laws saving that changes in the world’s power structure must end in war, despite all distur bances and ensuing risks (Rauch 2014). The less conflict an emerging power experiences with established ones, and with peer challengers that emerge simultaneously, the better the chances that the rise will travel a peaceful trajectory. Looking through this lens. thc relations of only one emerging power with the present hegemon appear to be partially conflict-pronc. and seriously so: it concerns the pair China/United States. The Iwo great powers are rivals for preponderance in East and South East Asia and eventually for being the number one at the global level. There is also Chinese resentment stemming from the US role in China’s past as a victim of Western imperialism. On the other hand. China’s authoritarian system of rule and ensuing violations of human and political rights trigger the liberal resentment discussed in the first part of this chapter. which is rooted particularly strongly in US political culture. The Chinese—US relationship is thus thc key to a peaceful. tense or even violent future at the world stage. A small group of major powers. Including the United States and China, is interconnected today by a complex conflict system. China has territorial claims against Japan, South Korea, Vietnam. the Philippines. Brunci. and India which it pursues by a variety of means, not shying away from the limited, small scale usc of militan force in some cases, notably against obviously weaker counterparts (Ellcman ci al. 2012). China’s relation (o wards Japan is the one most burdened by China’s past as a victim of Japanese oppression and related cruelties, and the propcnsit of the conservative part of Japan’s elite to display cavalier attitudes towards this past or even sort of celebrate it (as through visits to the notorious Yasukuni shrine hosting the remnants of war criminals) only adds to anti-Japanese feelings in China (Russia. another great power. also openly pursues a revisionist agenda. as vividly shown in the recent Crimean move, but these territorial ambitions are not part of the most virulent conflict complex in Asia). Territorial claims are always emotionalized and dangerous. Territorial claims by a major power bear particular risks, because threatened countries look for protective allies which are, by necessity, major powers with the capability to project power into the region of concern. The great power claimant and the great power protector then position themselves on the opposite sides of the conflict. A classical constellation of great power conflict results that looks far more traditional than all the talk about post-modern global relations in which state power struggles fade into oblivion would suggest. In the Asian conflict complex that structures the shape of the US—Chinese contest (Foot/Walter 201 1). Japan. South Korea and the Philippines arc for mall allied ith the United Slates. India and Vietnam today entertain rda (ions ith the United States that can be depicted as cordial entente, already include military cooperation, and might move further towards an alliance. depending on deelopmens in Asia. The United States is also a protector of Taiwan. officially a Chinese province, factualh an independent political entity. and the main object of Chinese interest because of the unfinished agenda of national re-unification. Given the enormous asymmetries between China and Taiwan. the latter’s independence depends fully and unambiguously on the US guarantee. Russia and China have a fairly ambivalent relation with each other that is officially called a strategic partnership. Ambiguous as this relationship is, it is predictable that the more the West and Russia are at loggerheads, the closer the Russian—Chinese relations might become. On the other hand. Chi na is the stronger partner and harbors not completely friendly feelings to wards Moscow. as Russia took part in China’s humiliation during the imperi alist period no less than the United States did. Russian fears concerning covert immigration into Eastern Siberia and demographic repercussions and political consequences that might result therefrom add to the uneasiness. China and India arc natural rivals for regional preponderance in Asia (Gilbov/Hcginbotham 2012). Both arc developing rapidly. with China still ahead. Territorial disputes. India’s liospitalit Lo TibeLan exiles including the Dalai Lama. China’s close relation to Pakistan and a growing naval rivalry spanning the Indian Ocean from the Strait of Malacca to Iranian shores (Garofano/Dew 2013) run parallel to rapidly growing economic relations and ostensible efforts lo present the relationship if not as amiable then at least as partner-like. The United States, China, Russia and India even today conduct a multi- pronged nuclear arms race (Fingar 2011: Gangul /Thompson 2011: O’Neill 2013. Müllcr 2014). In this race, conventional components like missile de fense. Intercontinental strike options, space-based assets and the specter of cbcr war play their role, as does the issue of extended dcterrcncc The general US militar’ superiority induces Russia and China to improve their nuclear arsenals, while India tries not to be left too far behind the Chinese in terms of nuclear capability. Pakistan and North Korea ork as potential spoilers at the fringe of this arms race. They are not powerful but thc arc capable of stirring up trouble, whenever they move. In tems of the military constellation, the most disquieting development is the drafting of pre-emptive strategies of a first (most likely conventional) strike by the United States and China, on either side motivated by the per ceived need to keep the upper hand early in a potential clash close to Chinese shores (such as in the context of a Taiwan conflict). China is building up middle-range ballistic capabilities to pre-empt US aircraft carrier groups from coming into striking distance and to desiroy US Air Force assets in Okinawa. while the United States is developing means to neutralize exactly these Chinese capabilities. They are steering towards a hair-trigger security dilemma in which the mutual postures cry out for being used first before the enemy might destroy them (Goldstein 2013: Le Miôre 2012). It cannot be excluded that this whole conflict system might collapse into two opposing blocks one da the spark for a major violent cataclysm could even be lighted by uncontrolled non-state actors inside some of the powers. or—in analogy to the role of Serbia in 1914— a ‘spoiler” state with a particularly idios ncralic agenda. Pakistan. North Korea or Tai an arc con ceivable in this role. Even Japan might be considered, if nationalism in Nippon grows further and seeks confrontation with the old rival China. If anything. this constellation does not look much better than the one which drove Europe into World War I a century ago. and it contains a nuclear component. To trust in the infallibility of nuclear deterrence in this mufti- pronged constellation needs quite a lot of optimism Can democratic peace be helpful in this constellation? Our conflict system includes democracies—the United States, India, Japan. Indonesia and non- democracies such as China. Russia, and Vietnam, but not necessarily on the same side. Should the European theater become connected to the Asian one through continuous US—Russian disputes and a Russian—Chinese entente. defective democracies like Ukraine and Georgia may feature rather importantly as potential triggers for a worsening of relationships. While democracy is useful in excluding certain conflict dyads in the whole complex, such as India and the United States. Japan and the United States. Japan and India. from the risk that they might escalate into a violent conflict, and as democratic peace is pacifying parts of the world. such as South America or Europe. it helps little in disputes between democracies and non-democracies. To the contrary: as discussed above, democracies have a more or less moral-emotional inclination to demonize non-democracies once they dis agree, and to feel a missionary drive to turn them democratic. This might exacerbate the existing, more interest-based conflicts between democracies and non-democracies, and it creates fears in the hearts of autocratic leaders that they might be up for democratization sooner or later. The close inter- democratic relations which democratic peace tends to produce, in turn, only exacerbate these fears as democracies tend to be rich, well organized, and powerful and dispose together of much more potent military capabilities than their potential non-dcnwcratic counterparts. Rather than helping with peace. the inter-democratic consequences of the democratic peace tend to exacerbate the security dilemma which exists between democracies and non-democracics an way. This non-peaceful dark side of democratic peace has escaped the attention of most academic writings on this subject and certainly all political utterances about democratic peace in our political systems. But democratic militancy is the Siamese twin of democratic peace as the Bush Administration unambiguously taught us (Gels et al. 2013: Müllcr 2014b).

#### 2. Median voter theory – democracies fight capital intensive wars more frequently.

Caverley 10 – Jonathan, Poli Sci Prof @ NU, The Myth of Military Myopia: Democracy, Small Wars, and Vietnam, International Security 34.3.

This section offers a theory of how a rational actor, the average voter in a democracy, can favor what appears to be a nonstrategic policy. To do so, it uses the core logic of a research program claiming that this sort of behavior should rarely happen in democracies. The theory presented here shares three impor- tant assumptions with the cost-internalization logic of democratic exception- alism: the distribution of costs within the state affects its pursuit of security; a democratic government's provision of security is a public good; and voters "take a reasonably level-headed cost-benefit approach in forming attitudes to- wards military missions."28 I relax the claim that costs are always internalized within democracies, however, arguing that the average voter's share may be much lower than the state's per capita costs. Even in democracies, wealth is not distributed equally within any given state; the person with median income is less well off than someone possessing the mean. A political-economic approach, the Meltzer-Richard hypothesis, suggests that if the median voter can set a tax rate and spend the revenue on a service available to all citizens, she will take advantage of the potential for re- distribution.29 Even with a flat tax on income, the wealthy will pay a larger portion of the costs for a public good enjoyed by all. For example, in 2005 the fifth of the population with the highest incomes paid 69 percent of all U.S. fed- eral tax revenue, and the middle fifth paid only 9 percent.30 Similarly, the median voter will prefer to tax capital more heavily than labor, because labor income is distributed more equally than capital income.31 How these taxes are spent plays a most important role in establishing the redistributive nature of the public good of defense. Military doctrine, the means by which military power is developed and exercised, can be stylized as a production function consisting of two factors - capital (e.g., tanks, planes, ammunition, and even training) and labor (soldiers, sailors, etc.) - as well as the technology that allows one factor of production to serve as a substitute for another.32 Capital and labor are imperfect replacements and show diminishing returns; given a hundred tanks and ten soldiers, adding another tank will not produce as much capability as adding another soldier. The type of conflict af- fects substitutions as well; it is much harder to substitute capital for labor when fighting an unconventional opponent. Tax revenue can pay for both the capital and labor inputs. Personnel also can be supplied through conscription, a tax on a citizen's labor rather than income. Even if the odds of being conscripted are equally distributed, the median voter will demand that a larger amount of the military budget go toward the purchase of capital to reduce the risk of conscription. In cases where existing threats do not currently justify resorting to conscription, military capitalization will still to a large degree determine a draft's future likelihood. The median voter normally will be happy with an expensive, all-volunteer military; but once the level of threat creates a demand for labor that reaches into the middle class, the voter will support a conscripted military where draftees are protected by large amounts of capital.33 Casualties are also a public bad: no one wants to see their fellow citizens die. The less wealthy are more likely to be drafted and to join an all-volunteer force; they may gain jobs from domestic weapons manufacturing; and they of- ten regard military service as a means of acquiring human capital. Conscription is therefore an important, but not the only, reason why militaries with large amounts of labor can be a public bad. The median voter will accept a higher tax, what the British socialist Sidney Webb called the "conscription of riches," to build highly capitalized militaries both in peace and in war, because such militaries redistribute money and skills through jobs and training as well as reduce the risk of conscription and casualties. The median voter theory outlined above does not claim to perfectly capture how policy is made in a democracy, nor does it argue that one's relative in- come determines one's position on foreign policy. Rather, this simple theory suggests an equally simple insight: a military doctrine that privileges capital over labor will reduce the costs of conflict for an important swath of voters. A capitalized military not only results in many voters doing less of the fighting themselves, but also allows someone else's resources to fund the costs of war. Politicians should respond accordingly. This distribution of costs explains how a state's seemingly nonstrategic behavior may be in the interests of important rational actors within a democracy. Because of its redistributive nature, a capitalized military doctrine can lead to moral hazard, which arises when perverse incentives encourage actors to pursue risky behavior. For example, drivers with auto theft coverage are more likely to park on the street than pay for secure parking. Many domestic gov- ernment programs merge moral hazard with the Meltzer-Richard effect dis- cussed above. Deposit insurance uses government backing to insure bank deposits up to a certain limit, a redistributive public good. Because the insur- ance applies regardless of the bank (subject to government regulations), an individual has little motivation to consider the bank's solvency. Indeed, she is likely to choose the higher interest provided by a bank making risky investments. Regarding defense provision, a lack of cost internalization creates an incentive for the median voter to support risky behavior: that is, using a capital- intensive military in conflicts where substitutability is low because the decreased likelihood of winning is outweighed by the lower costs of fighting in such a manner. If the median voter's risky behavior is in effect being subsidized by the wealthy, democratic leaders sensitive to this voter's costs will pursue strategies that make success less likely. I argue that this is what happened in Vietnam.

### Ext --- Democracy Bad

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

Chiba 21 --- Dr. Daina Chiba, 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.

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

Chiba 21 --- Dr. Daina Chiba, 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.

#### US and Israel prove – citizen preferences for a capital-intensive military doctrine lock in aggressive foreign policy and protracted warfare – legal reforms fail.

Caverley 10 – Jonathan, Poli Sci Prof @ NU, The Myth of Military Myopia: Democracy, Small Wars, and Vietnam, International Security 34.3.

This article shows that, contrary to the consensus regarding U.S. military intransigence in the face of unconventional warfare, civilian officials in Lyndon Johnson's administration - and ultimately the American public - played an essential role in the selection of a capital-intensive strategy to fight insurgents in the Vietnam War. President Johnson was convinced that the American public would punish any administration that "lost" South Vietnam to communism, but he was equally certain that public preferences constrained the number of U.S. forces to be deployed and lives to be lost far more than the amount of money to be spent and ordnance to be consumed. In response, he and his sub- ordinates instructed the military to fight what they themselves acknowledged to be an ineffective, capital- and firepower-intensive strategy. The article ex- plains this seemingly nonstrategic behavior using a theory, generalizable be- yond this specific case, of the distribution of the costs of war within the electorate.138 Israel's experience in its 2006 war against Hezbollah suggests that this phenomenon is not limited to the Vietnam War or to U.S. strategic culture.139 Israel expended 170,000 artillery shells, twice the number fired in the conve tional 1973 Arab-Israeli War, in a month.140 The Israel Defense Force's (IDF's) initial campaign plan - a rapid air and small-unit ground assault that relied on firepower to control territory - was designed to minimize the number of ground forces and casualties. The Israeli cabinet rejected it; the transportation minister objected to "exposing 40,000 troops to the Lebanese reality."141 Four days into the conflict, the IDF deputy chief of staff recommended stopping the campaign: "We have exhausted the [aerial] effort; we have reached the peak; from now on we can only descend."142 Nonetheless, despite its intention to avoid a ground war, the Israeli government announced ambitious goals far beyond releasing hostages and deterring further rocket attacks.143 A report written by a subsequent government commission describing the strategic co- nundrum evokes the constraints faced by Johnson in Vietnam: "Declared goals were too ambitious, and it was publicly stated that fighting will continue till they are achieved. But the authorized military operations did not enable their achievement." The report acknowledges the government's bind: no "other ef- fective military response to such missile attacks than an extensive and pro- longed ground operation" existed, but this "would have a high 'cost' and did not enjoy broad support."144 Cost distribution theory makes such behavior explicable. From four ma- jor assumptions - security is a public good; voters weigh security benefits against taxes, conscription, and casualties; median wealth is less than mean wealth in every state; and the preferences of the median voter are heeded in a democracy - I derive a voter preference for a capitalized military. Like the democratic exceptionalist research program, this article finds evidence that the American public weighs the benefits of limited war against the costs. Although one recent study of American public opinion assigns expectations of success as the most important factor in the public's support for a conflict, it also points out that the public more generally carries out relatively competent cost-benefit analysis.145 This article extends this logic by arguing that when the ability to substitute matériel for personnel is low, as it is against unconventional opponents, democracies may still prosecute wars using an ill-suited military doctrine (and thus a lower chance of success), because the costs remain modest for this pivotal voter. Democratic exceptionalism's cost-internalization mechanism provides an overly optimistic assessment of democracies' discretion in how and even when they fight small wars. Neither an apolitical public, nor a dysfunctional military culture, nor a military doctrine divorced from grand strategy causes a flawed warfighting strategy. Rather, it results from political leaders' assessment of the average voter's preferences. Although claiming that democracies substitute capital for labor to reduce the costs of war for voters is not news, tying the pur- suit of such a strategy to a rational voter has two novel and important implications. First, many observers argue that most wars of the twenty-first century will be hybrid conflicts involving unconventional opponents; finding the root cause of poor counterinsurgency is an essential task. This article argues that fixating on reforming the armed services (or even the civilian tools of foreign policy) in an effort to improve democratic performance in small wars is its own form of myopia. My theory gives reason to be skeptical of how much the U.S. military will be allowed to shift by future administrations and the public to which they are held accountable. Dysfunctional organizations can eventu- ally learn and adapt. If the public suffers from foolish preconceptions, it may be dissuaded through public education and the marketplace of ideas. Even positing a powerful strategic culture underpinning U.S. doctrine suggests that "it is at least possible that by deconstructing the standard American 'way' . . . some pathways to improved performance may be identified."146 But if a rational, fully informed electorate views such a military doctrine as its best option, the prospects for change are less clear.

## A2: Solvency

### 1NC --- Say No

#### No modeling --- countries don’t want to share their cyber secrets

Jacobsen 20 --- Jeppe T Jacobsen, Ph.D. candidate at the Danish Institute for International Studies and the University of Southern Denmark, “Cyber offense in NATO: challenges and opportunities”, International Affairs, Volume 97, Issue 3, May 2021, Pages 703–720, https://academic.oup.com/ia/article-abstract/97/3/703/6205395

The third challenge to the integration of cyber effects in NATO operations relates to a well-known military concept, deconfliction. The coordination by allies and military units of their efforts to avoid confliction, between for example an air operation and a special forces operation in the same area, is a central element in every military campaign. Deconfliction is all about openness and communication between allied partners. But in cyberspace, deconfliction comes with several difficulties. At the core of these difficulties is the fact that the tools and techniques that produce cyber effects—which are often also used and heavily depended on for intelligence collection—are developed in secret and must stay secret until the effect is achieved. If the IT vulnerabilities and exploits are known, vendors or adversaries can fix or replace the software and thereby render the effect impossible to achieve.39 In an alliance not known for sufficient mutual trust among members to share intelligence,40 there is little indication that allies will become more open about the cyber tools and techniques they currently have at their disposal. The request-based model is the result of that lack of trust. And the unwillingness to share cyber intelligence seriously challenges NATO’s ambition to use CYOC to facilitate information-sharing to increase situational awareness and thereby achieve the ‘cyber readiness’ and ‘cyber resiliency’ that NATO Deputy Secretary-General Mircea Geoană hopes to attain.41

### Ext --- Say No

#### No sharing

Borghard & Lonergan 19 --- Erica D. Borghard Adjunct Research Scholar in the Arnold A. Saltzman Institute of War and Peace Studies, Saltzman Institute of War & Peace Studies, and Shawn W. Lonergan, Instructor in the Department of Social Sciences at the United States Military Academy at West Point and a PhD Candidate, “Cyber Operations as Imperfect Tools of Escalation “, STRATEGIC STUDIES QUARTERLY FALL 2019, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13\_Issue-3/Borghard.pdf

Second, beyond operational requirements for secrecy, states make political decisions to eschew attribution for offensive cyber operations.64 States employ technical methods to avoid attribution (e.g., obfuscating points of departure of attacks by using spoofing, proxy servers, third-party infrastructure, compromised certificates, and other anonymizing capabilities) as well as make deliberate efforts to obscure command and control for cyberattacks (e.g., using cyber proxies with varying degrees of plausible deniability).65 The time requirements for a targeted state to achieve attribution at a reasonable confidence threshold, as well as its willingness to share potentially sensitive intelligence information with allies or domestic publics to justify any escalatory responses, create additional temporal breaks for the pressure of a crisis situation to diffuse and for decision-makers to evaluate alternative courses of action.

#### NATO wont share

Herpig & Reinhold 18 --- Sven Herpig, PhD, project director for international cyber security policy, and Thomas Reinhold, research associate and PhD student at the Department of Science and Technology for Peace and Security (PEASEC) at TU Darmstadt“Spotting the bear: credible attribution and Russian operations in cyberspace”, European Union Institute for Security Studies (EUISS) (2018), https://www.jstor.org/stable/pdf/resrep21140.7.pdf

Although crucial to solving the challenge, the intelligence component has been the most underrated aspect in the public debate. The reason for that is the classification of intelligence materials and thus their rare exposure to public scrutiny. After the US presidential elections in 2016, the American intelligence community issued a declassified intelligence report18 that was supposed to convince the public of Russia’s guilt. It however achieved almost the opposite effect because – due to declassification – the public report no longer contained any hard proof of Russian intervention. When asked whether they think Russia attempted to meddle in the 2016 presidential elections, 45% of respondents in the US answered either that they do not know or that it is not true.19 At the end of the day, it is the state’s strategic choice how much it discloses about what it knows and how it obtained its intelligence. Therefore, credible attribution is indeed within the realms of possibility. Whether that proof can be presented to international organisations (e.g. UN, NATO) and/or the public or not is a different story as this would likely mean exposure of the intelligence operation. Revealing such an intelligence operation would decrease the likelihood of it still being effective in the future. If attackers follow the counter-response to their actions closely, they might be able to identify what measures were used to track them down and circumvent/avoid them if possible.

# \*\*Off-Case\*\*

## Topicality --- Security Cooperation

#### Information sharing is distinct from cybersecurity

Zaccor 05 --- Colonel Albert Zaccor U.S. Army Atlantic Council Senior Fellow, “Security Cooperation and Non-State Threats: A Call for an Integrated Strategy”, The Atlantic Council, August 2005, https://www.files.ethz.ch/isn/46290/2005\_08\_Security\_Cooperation\_and\_Non-State\_Threats.pdf

Relationships built on trust and mutual interests are also necessary to obtain cooperation from foreign governments in the area of Intelligence and Information. It is useful to separate the distinct, but related, issues of Intelligence Sharing and Intelligence Security Cooperation. Intelligence Sharing is a critical element in the fight against non-state threats, or strategic crime. By its nature, however, such sharing involves sensitive sources, methods and arrangements, normally in the context of a bilateral relationship. Its sensitivity requires delicate handling in highly restrictive channels. Intelligence sharing, in practice, falls outside the scope of Security Cooperation. Intelligence Security Cooperation, on the other hand, involves the development of interoperable and cooperative intelligence systems and processes designed to enhance the ability of one partner to work with one or several other partners. The core activities in Intelligence Security Cooperation are analytical and expertise exchanges, familiarization, training, and traditional Security Assistance. Both Intelligence Sharing and Intelligence Security Cooperation are mutually supporting. It is clear that the quality and reliability of intelligence we get from our partners depends on the competence, capability, professionalism, and trustworthiness of their national intelligence services and how compatible their operations are with ours. Intelligence Security Cooperation provides the tools to develop long-range relationships with foreign partners to improve both the quality of the intelligence we share and our ability to work together.

## Disad --- Disclosure Bad

### 1NC

#### US Cyber capabilities are high but China is catching up

Marks 21 --- Joseph Marks, Anchor of The Cybersecurity 202 newsletter, Washington Post, “The Cybersecurity 202: The United States is still number one in cyber capabilities”, June 2021, https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/

The United States remains by far the world’s most cyber-capable nation with no major competitors for the title.

That’s the conclusion from a mammoth 182-page report released today by British think tank the International Institute for Strategic Studies that reviews the cyber capabilities of 15 of the world’s biggest players in hacking and digital defense. The report assesses both government and private-sector capabilities.

The report relegates the most troublesome U.S. adversaries, Russia and China, to a second tier of cyber powers. That group also contains the United Kingdom, Canada, Australia, Israel and France.

However, China’s rapid digital development and its growing slate of technology firms make it “the only state currently on a trajectory to join the U.S. in the first tier of cyber powers,” the authors warn.

The report marks a major endorsement for U.S. cyber capabilities, which have been called into question by a string of major cyberattacks by Kremlin-linked hackers and Russia-based cybercriminals. It also comes as U.S. officials are struggling to temper the global growth of Chinese tech firms, which they fear could give Beijing a critical edge in cyber competition.

“China has made significant progress in bolstering its capabilities since 2014, but nowhere near enough to close the gap with the U.S.,” said IISS Senior Fellow for Cyber, Space and Future Conflict Greg Austin. “The main reason is the relative standing of the two nations’ digital economies, where the U.S. remains far advanced despite China’s digital progress.”

#### Sharing vulnerabilities weakens the United States cyber-capabilities --- China will exploit

Aitel & Rampersaud 14 --- Dave Aitel is CEO of Immunity Inc., a leading offensive security firm that serves major financial institutions, industrials, Fortune/Global 500s and US government/military agencies. He is a former NSA computer scientist and DARPA contractor. Skylar Rampersaud is a former NSA computer scientist and director of vulnerability analysis at Immunity., “Some People Want A Time Limit On The NSA's 'Zero-Day' Exploits — Here's Why That's A Terrible Idea”, Jul 2, 2014, https://www.businessinsider.com/why-a-time-limit-on-zero-days-is-a-bad-idea-2014-7

In particular, people have suggested that the NSA be restrained from collecting a “zero-day” stockpile and that one of the logical ways to do this was to force them to report any discovered vulnerabilities to the vendor for patching after a certain time period has elapsed, presumably so they could use them in the meantime for intelligence collection.

First, some context from the White House’s NSA task force and their own blog:

Recommendation 30: “US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency review involving all appropriate departments.”

“But there are legitimate pros and cons to the decision to disclose, and the trade-offs between prompt disclosure and withholding knowledge of some vulnerabilities for a limited time can have significant consequences. Disclosing a vulnerability can mean that we forego an opportunity to collect crucial intelligence that could thwart a terrorist attack stop the theft of our nation’s intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks.”

However, people with experience in the field of information operations, computer and network exploitation, or any related signals intelligence occupation know that assigning a time limit to your methods is madness.

Specifically, computer and network operations are fragile in the sense that they are often linked together. Take one simple sample operation for example: penetrating the Iranian nuclear establishment.

This may involve at a minimum three different kinds of 0days (penetrating into a computer, taking full control of that computer, and spreading from that computer to other computers), but it also involves special software for maintaining a presence on the network and getting large volumes of data out of the network (think FLAME). These tools are known as “implants.”

Obviously, the first time someone discovers the implant, they can hunt down all other machines that have been infected and start making guesses as to what information you were after, or may have gotten. This is why the minute you become aware that someone has found you, you clean up every possible operation using that implant.

What is less well known is how the discovery of vulnerability information (“0days”) can affect operations. In particular, the modern age of cloud computing allows countries to store and analyze huge volumes of their traffic (or indeed, other countries’ traffic, as Snowden has helpfully pointed out). This means that when a vulnerability goes public they can search through all of history to find out when any traffic matching that vulnerability may have happened. They then rush to look at that machine, and will likely find any implant on it.

In other words, releasing a vulnerability means that all of your implants in Iran must be removed if any of them were installed using that vulnerability. In addition, hard targets are often compromised with the help of human agents, recruited by human intelligence organizations. These people’s lives are then put at risk if any computer they have touched is discovered to have been compromised by a tool that can be linked back to the United States or her Allies.

In addition, you are not just releasing the information that the vulnerability exists. If you are giving that vulnerability information to the vendor, you are also saying that it was definitely the United States government that was involved with that operation. This solves the “attribution problem” for your enemy.

But it solves more difficult problems for your enemy too. Software bugs are often related, and the knowledge that a bug exists can lead them to find different bugs in the same code or similar bugs in other products. By looking at all the vulnerabilities you release, they know the state of your vulnerability-finding programs. They know how far ahead or behind of you they are. They can focus their own vulnerability-finding resources with greater precision. They will be able to find vulnerabilities that you have not found - and they will have the added advantage of knowing when to wrap up their own exploit operations.

Vulnerabilities are a finite thing - taking the tack of releasing them over time means that eventually the United States’ ability to find them will be heavily drained, but China’s will not, much like exhausting an oil reserve.

Even if we ignore the problem of adversarial nation-states gaining an advantage in vulnerability research, the discussion of a limited-use window appears based on a non-existent thing: a static set of intelligence priorities. The idea being presented is that the NSA would find a vulnerability, use it for some amount of time to exploit its “high priority” intelligence targets, then send it off to be patched.

This ignores the fact that intelligence priorities can change rapidly and often, hindering NSA’s ability to respond rapidly to world events. In addition, computer network operations are continuous things that often involve waiting for windows of opportunity--something that is incompatible with many of your tools having a time-limited lifespan.

Integrating 0days into a toolkit, testing them and using them may cost millions of dollars before it pays off with valuable intelligence. Keep in mind as well, that not all 0days pay off, and any can be discovered and destroyed in an instant and you have the very picture of a resource you can’t afford to waste.

Because of the interconnected nature of the entire computer and network exploitation framework, forcing the NSA to report vulnerabilities to vendors would force it to give up using vulnerabilities altogether. This is not a considered and wise action, even in light of Snowden’s revelations.

#### Loss of offensive capabilities, particularly zero-days, causes China to invade Taiwan

Ramos 21 --- Capt Allison R. Ramos Squadron Officer School Class 21-D, Flight B-19, “Cyber Deterrence: Controlling Escalation in Taiwan”, Website created Sept 17th 2021, https://www.airuniversity.af.edu/Portals/10/ISR/student-papers/AY21-22/CyberDeterrence\_ControllingEscalation\_Ramos.pdf

The Deterrence Operations Joint Operation Guide (DOJOC) defines deterrence as the ability to “Convince adversaries to not take action that threaten US vital interests by means of decisive influence over their decision making … [to] change the decision calculus of an adversary by denying benefits, imposing costs, or encouraging adversary restraint.”13 One method to deter is the cyber domain is through a forward-deployed presence. The US Cyber Command (USCYBERCOM) has included the concept as a central focus through superiority through persistence.14 The goal is to deploy as close to the adversary activity as possible, allowing the research of weaknesses, intentions, capabilities, and ability to counter-attack.15 USINDPACOM reinforces a cyber alliance with the ROK, Japan, and Australia to include information sharing and cyber attack response commitments.16 It lists the Philippines as a nation that the US will support specifically in an armed attack in the South China Sea.17 However, it does not mention Taiwan or cyber attacks. Forward deploying in cyberspace assumes that the US can act in cyberspace while controlling escalation and the persistence will deter others from cyber attacks.

Forward deployed troops allow for the normalization of cyber operations, which decreases the risk of escalatory response in a conflict situation. The decision to forward deploy in cyberspace includes cyber protection teams, operations within allied networks, operations against adversary networks, intelligence sharing with allies and partners, and using malware to set up critical national infrastructure to be effected.

The US must forward deploy troops because of the organizational decision to support Taiwan. The 2017 National Security Strategy included Taiwan and stated the US would provide for Taiwan’s legitimate defense needs and help deter coercion.18 The Interim National Security Strategy Guidance reaffirmed that guarantee, including comments that Taiwan is a democracy and critical economic and security partner in line with American commitments.19 The US values democracy, human rights, and human dignity as the basis for all top-level doctrine and strategies. Each document includes spreading and securing democracy as part of its core mission. In a cyber event with China, China could stifle the fundamental right to freedom of information or speech through a DDoS attack as was seen in Hong Kong or a zero-day attack that could have strategic-level effects on critical national infrastructure. The US must deter Chinese aggression towards Taiwan as aligned with their diplomatic pledge.

#### Taiwan invasion causes nuclear war

Walker, 9-18-2020, Richard Walker reporter for Deutsche Welle Deutsche Welle (DW) is Germany’s international broadcaster and one of the most successful and relevant international media outlets. DW is an unbiased media organization, based in Germany. We provide our journalistic content to people worldwide, giving them the freedom to make up their own minds and the information required to form their own opinions, Taiwan: The threat that the world ignores," DW, https://www.dw.com/en/taiwan-the-threat-that-the-world-ignores/a-54944934, Accessed: 1-21-2021, MB

Taiwan's Foreign Minister Joseph Wu is ringing the alarm, hoping that the world will pay attention to the profound threat emanating from China.

"The threat is very real and therefore Taiwan's preparation is also very serious," he told DW. "We are trying to deal with the military threat, day in and day out."

China's aggressive military probing has been going on for years — an unending stress test for the democratic island it claims as its territory.

But in 2020, the threat has taken on a new intensity. Over and over again, Taiwan has had to scramble fighters to intercept Chinese warplanes flying towards or even into Taiwan's airspace.

With China cracking down on freedoms in Hong Kong, accused of sweeping repression against the Uighurs in Xinjiang, expanding in the South China Sea, and clashing with India in the Himalayas, Taiwan is asking: Are we next?

In a new in-depth film DW lays bare the risks to this highly vulnerable and yet thriving society, and examines three possible scenarios with strategy and military experts from Taiwan, China, the US and Germany.

The underestimated threat

China is completely open about the threat. President Xi Jinping framed it himself in a high-profile speech in 2019: "We do not promise to renounce the use of force and reserve the option to use all necessary measures."

Yet this threat to Taiwan receives little international attention.

"To say that the world has underestimated the severity of this flashpoint and that there's the potential for war over Taiwan — I think itself is an underestimation," said Ian Easton of the Project 2049 Institute in Washington, DC, and author of "The China Invasion Threat."

James Fanell, former intelligence chief for the US Pacific Fleet, agrees: "2020 to 2030 is the most dangerous time on earth, in my opinion, for a conflict with China over these disputed territories."

Taiwan exposed

Despite flourishing into a vibrant, high-tech democratic society since its split from mainland China at the end of the civil war in 1949, Taiwan is highly exposed.

Just 15 countries around the world recognize it as an independent state. It is frozen out of international bodies like the UN and the World Health Organization. And with a population of under 24 million, it is dwarfed by China.

Crucially, the military gap between China and Taiwan widens every year.

Washington supplies Taipei's armed forces in line with defense commitments made after it switched diplomatic recognition to Beijing in 1979. But those commitments are highly ambiguous. They stipulate that Washington maintain "the military capability in the West Pacific to prevent intimidation and coercion against Taiwan," said Bonnie Glaser of the Center for International and Strategic Studies in Washington, DC.

"Notably, that is not a commitment to come to Taiwan's defense in the event that it is attacked," Glaser said.

China's military might

China's threat to Taiwan is backed by vast military power. It has spent decades amassing the resources to follow through — pouring massive investment into its naval forces, even overtaking the US.

"For the last five years plus, they've been producing literally five times as many ships per year as the US Navy produces," said former Intelligence Chief James Fanell. "My projection is that the Chinese Navy by 2030 will have over 550 ships and submarines, and the United States Navy is still struggling to figure out how to get to 350-355."

Key here is not only the size of the fleet but the type of ships Beijing is building and the forces that work with them. China's new generation of amphibious warfare vessels, coupled to an expanded marine corps, would play a critical role in a possible invasion of Taiwan.

Outgunning the United States

China's array of anti-ship missiles is another part of the arsenal. "They've developed this cornucopia of missile systems designed specifically to defeat our Navy," said Fanell.

China is the world leader in this technology. "They have anti-ship cruise missiles like the YJ-18, which has a range that's longer than anything that the United States has right now," said Fanell. "And they have anti-ship ballistic missiles that were specifically designed to go after US Navy aircraft carriers."

These weapons are precisely what China would need to deter — or repel — a US intervention to defend Taiwan.

"Even five years ago, the ability of the United States to come to Taiwan's defense was greater than it is today," said Bonnie Glaser. "It has eroded over the last decade. And that is, I think, problematic."

Scenarios

So what could actually happen?

In the new film DW examines three possible scenarios in detail: gradually chipping away at Taiwan's stability via military and hybrid means; a sudden, Crimea-style annexation of outlying islands; and finally a full-scale invasion.

An invasion would involve enormous risks not just to Taiwan, but to the whole world. The US would face the dilemma of whether to intervene — potentially sparking a war between two superpowers.

"Everything that happens in this scenario happens under the shadow of a potential nuclear war," Easton told DW. "Every decision that was made every minute, every day of a crisis or once a crisis escalates to war; you would never know when things could spin out of control."

The world is not ready

Ian Easton says that this last, most dangerous scenario could arise from internal turbulence in China.

"You could imagine all kinds of disasters that that could occur that would put pressure on the central leadership to get people to rally around the flag. And of course, at that point, Taiwan is an obvious one, especially if it's not clear that the United States is committed to Taiwan's defense."

A period of political instability in the US — such as a contested presidential election result as feared this year — could open a window of opportunity. And Taiwan's foreign minister, Joseph Wu, warned that conditions could converge in China sooner than many expect.

"If you look at the internal situation in China at this moment, the economy has been affected by COVID-19 and also the very serious floods," he said. "Under these kinds of circumstances, the Chinese authoritarian leaders may find Taiwan as a convenient scapegoat. Therefore Taiwan needs to be doubly concerned about a possible Chinese use of force against us."

### Overview

#### Disad turns and outweighs the case – Over-sharing discloses vulnerabilities that adversaries can exploit --- also limits capabilities for conducting OCOs --- the impact is China war --- US cyber dominance is key to deter a Taiwan invasion --- weakening US position through unilateral disclosure gives China tactical advantages that they will exploit

#### Unwanted nuclear escalation is likely---comingled systems AND irrationality.

Sweeney 21 --- Mike; March; Fellow at Defense Priorities; Defense Priorities, “Why A Taiwan Conflict Could Go Nuclear,” https://www.defensepriorities.org/explainers/why-a-taiwan-conflict-could-go-nuclear]

The preferred U.S. style of warfare—to conduct attacks deep throughout an enemy’s territory rather than simply meeting them at a forward line of engagement—also presents problems and contains the prospect that non-nuclear strikes might unintentionally trip Chinese redlines regarding nuclear use. Within the U.S. academic community, this has produced a small, but important body of literature focused on the subject of “entanglement,” or the co-mingling of systems with both conventional and nuclear applications.48 This discussion has primarily focused on China’s ballistic missile force, as most of its systems are capable of firing both nuclear and non-nuclear warheads.49

China’s increasing reliance on road-mobile ICBMs (such as the DF-31 variants and the new DF-41) complicates this problem, creating the potential for their misidentification as shorter-range systems, such as the road-mobile DF-21 and DF-26, that might be used against U.S. ships or regional bases.50 Analysts have also expressed concern over the potential for U.S. forces to inadvertently sink a Chinese SSBN as part of its ASW campaign during a Taiwan conflict, a fear that echoes similar worries from the U.S.-Soviet struggle.51 Recall again the private comments of Chinese officials about conventional attacks on nuclear systems nullifying its NFU policy.

THE POTENTIAL FOR MUTUAL MISCALCULATION

Entanglement issues are far from the whole of the problem. There is still a fundamental misreading—perhaps on both sides—of the ability to manage escalation in Taiwan contingencies for reasons beyond strict operational matters. The very fact of China attempting something as complex and challenging as an amphibious invasion of an island of 24 million people would show an unwelcome tolerance for risk. For that matter, U.S. efforts to defend said island—halfway around the world on another nuclear power’s doorstep—also shows a fair amount of audacity. Put differently, the act of aggression against Taiwan and the effort to repel such an attack both demonstrate that each side is willing to take actions which could be viewed as inherently risky.

Through that lens, the additional step to unwanted nuclear escalation is not a great leap. States act rationally, right up until they do not. In considering how a Taiwan contingency would play out, it would therefore be prudent to assume that nuclear use is more viable than cold assessments of each side’s pre-conflict intentions suggest. If academic surveys of Chinese strategic literature are correct, overoptimism on the ability to manage escalation once hostilities commence is not confined to the U.S. side.52

#### Goes nuclear.

Warren 21 --- James; July 22; visiting scholar in the American Studies Department at Brown University; the Daily Beast, “Wonder Where World War III Might Break Out? Try Taiwan,” https://www.thedailybeast.com/wonder-where-world-war-iii-might-break-out-try-taiwan]

Ever wondered where World War III might break out?

A clear and troubling consensus has emerged in the American national security community that the Taiwan Strait is the most likely place for a major war to erupt between the United States and China; that it might start soon, and that such a conflict might quickly escalate into a nuclear confrontation.

In March, the leading foreign policy organization in the United States, the Council on Foreign Relations in New York, issued a report concluding that Taiwan has become “the most dangerous flashpoint in the world.” There, a unique and troubling set of geopolitical developments have conspired to make a shooting war between the People’s Republic of China and the United States more likely than ever before. Recently the newly appointed commander of U.S. forces in the Indo-Pacific Region, Admiral John Aquilino, remarked that a possible invasion of Taiwan by the People’s Republic of China (PRC) “is much closer than we think.”

#### Draws in everyone

Blackwill 21 --- Robert and Philip Zelikow; February; Deputy National Security Advisor under George W. Bush, Lecturer in International Security at Harvard; History Professor at the University of Virginia, Former Executive Director of 9/11 Commission; Council on Foreign Relations, “The United States, China, and Taiwan: A Strategy to Prevent War,” Council Special Report No. 90]

The horrendous global consequences of a war between the United States and China, most likely over Taiwan, should preoccupy the Biden team, beginning with the president. It could be unlikely that a U.S.- China conflict would go nuclear and Beijing has repeated its no first use doctrine, but there is little doubt that China wants to grow its arsenal of a few hundred warheads and build a more sophisticated force that could employ hypersonic glide capabilities.189 Millions of Americans could die in the first war in human history between two nuclear weapons states. A 2015 RAND Corporation study of the effects of U.S.-China combat determined that estimating military losses would be “exceedingly difficult.” World War II, however, was the last time the United States lost a major warship, and one sunk vessel could turn into the deadliest U.S. military event since the Vietnam War.190

The outbreak of a great power war would likely produce a global recession, if not a depression. It would disrupt Asian and international trade, sever major supply chains, and could collapse international financial systems.191 This would produce deeply painful economic consequences for U.S. allies, who trade more with China than they do with the United States. One study estimates that a single year of U.S.-China conflict could cause American GDP to decline by 5 to 10 percent.192

China could unleash cyberattacks on the United States. The New York Federal Reserve estimates that a major cyberattack on the U.S. financial system could cause 2.5 times daily GDP in forgone payments, and a Lloyd’s of London and Cambridge University study predicted that a hypothetical blackout affecting fifteen states could cause $243 billion to $1 trillion in damages, as well as deaths resulting from disruption to health care, traffic, and industry.193

In 2013, hackers associated with the PLA reportedly tried to infiltrate companies that control U.S. critical infrastructure, including Telvent which provides remote access and holds blueprints to North and South American oil and gas pipelines.194 In 2019, researchers uncovered a suspected Chinese plot to access American utility companies.195 Additionally, in September 2020, a ransomware attack said to have originated in Russia hit U.S. hospitals during a coronavirus surge and forced doctors to switch to pen and paper record keeping and postpone certain medical procedures.196 The outbreak of U.S.-PRC conflict could see multiple cyber events hit U.S. society and its allies in rapid succession.197

While Washington and Beijing were trading blows, Russia could threaten the Baltics, increase its presence in Ukraine, or provide oil and weapon support to China.198 Iran would be unlikely to stand idle in the Middle East in such a crisis given U.S. attention directed elsewhere. Another factor is the allied dimension. In matters ranging from technology issues to criticism of China’s handling of Hong Kong, U.S. allies have sometimes been hesitant to support Washington when American rhetoric and actions are deemed too provocative or come with high economic costs.199 France and Germany refused to support the United States in the 2003 Gulf conflict. In a U.S.-China war, even Japan might not join the battle given its domestic politics and constitutional constraints and the United States could well fight alone, shattering its alliance system.

#### 1NC Aitel & Rampersaud says that maintaining the offensive use of zero-days allows rapid crisis response capabilities --- the impact is every major security threat

Berkowitz 8 --- research fellow at the Hoover Institution at Stanford University and a senior analyst at RAND. He is currently a consultant to the Defense Department and the intelligence community (Bruce, STRATEGIC ADVANTAGE: CHALLENGERS, COMPETITORS, AND THREATS TO AMERICA’S FUTURE, p. 1-4)  
  
THIS BOOK is intended to help readers better understand the national security issues facing the United States today and offer the general outline of a strategy for dealing with them. National [security policy](https://muhaz.org/security-assurance-policy-helper-saph.html)—both making it and debating it — is harder today because the issues that are involved are more numerous and varied. The problem of the day can change at a moment's notice. Yesterday, it might have been proliferation; today, terrorism; tomorrow, hostile regional powers. Threats are also more likely to be intertwined—proliferators use the same networks as narco-traffickers, narco-traffickers support terrorists, and terrorists align themselves with regional powers. Yet, as worrisome as these immediate concerns may be, the long-term challenges are even harder to deal with, and the stakes are higher. Whereas the main Cold War threat — the Soviet Union — was brittle, most of the potential adversaries and challengers America now faces are resilient. In at least one dimension where the Soviets were weak (economic efficiency, public morale, or leadership), the new threats are strong. They are going to be with us for a long time. As a result, we need to reconsider how we think about national security. The most important task for U.S. national security today is simply to retain the strategic advantage. This term, from the world of military doctrine, refers to the overall ability of a nation to control, or at least influence, the course of events.1 When you hold the strategic advantage, situations unfold in your favor, and each round ends so that you are in an advantageous position for the next. When you do not hold the strategic advantage, they do not. As national goals go, “keeping the strategic advantage” may not have the idealistic ring of “making the world safe for democracy” and does not sound as decisively macho as “maintaining American hegemony.” But keeping the strategic advantage is critical, because it is essential for just about everything else America hopes to achieve — promoting freedom, protecting the homeland, defending its values, preserving peace, and so on. The Changing Threat If one needs proof of this new, [dynamic environment](https://muhaz.org/dynamic-adaptation-of-parallel-codes-toward-self-adaptable-com-v2.html), consider the recent record. A search of the media during the past fifteen years suggests that there were at least a dozen or so events that were considered at one time or another the most pressing national security problem facing the United States — and thus the organizing concept for U.S. national security. What is most interesting is how varied and different the issues were, and how many different sets of players they involved — and how each was replaced in turn by a different issue and a cast of characters that seemed, at least for the moment, even more pressing. They included, roughly in chronological order, • regional conflicts — like Desert Storm — involving the threat of war between conventional armies; • stabilizing “failed states” like Somalia, where government broke down in toto; • staying economically competitive with Japan; • integrating Russia into the international community after the fall of communism and controlling the nuclear weapons it inherited from the Soviet Union; • dealing with “rogue states,” unruly nations like North Korea that engage in trafficking and proliferation as a matter of national policy; • combating international crime, like the scandal involving the Bank of Credit and Commerce International, or imports of illegal drugs; • strengthening international institutions for trade as countries in Asia, Eastern Europe, and Latin America adopted market economies; • responding to ethnic conflicts and civil wars triggered by the reemergence of culture as a political force in the “clash of civilizations”; • providing relief to millions of people affected by natural catastrophes like earthquakes, tsunamis, typhoons, droughts, and the spread of HIV/AIDS and malaria; • combating terrorism driven by sectarian or religious extremism; • grassroots activism on a global scale, ranging from the campaign to ban land mines to antiglobalization hoodlums and environmentalist crazies; • border security [and illegal immigration](https://muhaz.org/immigration-politics--cal-2013--starter-packet.html); • the worldwide ripple effects of currency fluctuations and the collapse of confidence in complex financial securities; and • for at least one fleeting moment, the safety of toys imported from China. There is some overlap in this list, and one might want to group some of the events differently or add others. The important point, however, is that when you look at these problems and how they evolved during the past fifteen years, you do not see a single lesson or organizing principle on which to base U.S. strategy. Another way to see the dynamic nature of today's national security challenges is to consider the annual threat briefing the U.S. intelligence community has given Congress during the past decade. These briefings are essentially a snapshot of what U.S. officials worry most about. If one briefing is a snapshot, then several put together back to back provide a movie, showing how views have evolved.2 Figure 1 summarizes these assessments for every other year between 1996 and 2006. It shows when a particular threat first appeared, its rise and fall in the rankings, and in some cases how it fell off the chart completely. So, in 1995, when the public briefing first became a regular affair, the threat at the very top of the list was North Korea. This likely reflected the crisis that had occurred the preceding year, when Pyongyang seemed determined to develop nuclear weapons, Bill Clinton's administration seemed ready to use military action to prevent this, and the affair was defused by an agreement brokered by Jimmy Carter. Russia and China ranked high as threats in the early years, but by the end of the decade they sometimes did not even make the list. Proliferation has always been high in the listings, although the particular countries of greatest concern have varied. Terrorism made its first appearance in 1998, rose to first place after the September 11, 2001, terrorist attacks, and remains there today. The Balkans appeared and disappeared in the middle to late 1990s. A few of the entries today seem quaint and overstated. Catastrophic threats to information systems like an “electronic Pearl Harbor” and the “Y2K problem” entered the list in 1998 but disappeared after 2001. (Apparently, after people saw an airliner crash into a Manhattan skyscraper, the possible loss of their Quicken files seemed a lot less urgent.) Iraq first appeared in the briefing as a regional threat in 1997 and was still high on the list a decade later—though, of course, the Iraqi problem in the early years (suspected weapons of mass destruction) was very different from the later one (an insurgency and internationalized civil war). All this is why the United States needs agility. It not only must be able to refocus its resources repeatedly; it needs to do this faster than an adversary can focus its own resources.

### Link Overview

#### Plan weakens US OCO capabilities --- Governments collect vulnerabilities to use in OCOs --- Plans disclosure allows adversaries to know what we know --- they’ll shore up their defenses and not disclose what they know --- creating asymmetrical advantages --- thats Aitel & Rampersaud

#### Disclosure wrecks our cyber-deterrent

Jardine 20 --- Eric Jardine Assistant Professor, Political Science, Virginia Tech, “Optimizing Cyber Deterrence”, In The Cyber Deterrence Problem, Aaron F. Brantly, ed. (New York: Rowman and Littlefield), page 87-104, 2020, https://osf.io/ns7b3

Given the clear offensive potential of zero-day vulnerabilities, governments actively collect these software flaws in order to build up their cyber-arsenals. In the US, for example, the National Security Agency (NSA) actively attempts to identify and collect zero-days for the purpose of tailored access operations (TAO). In 2013 alone, the NSA reportedly spent $25 million purchasing zero-day vulnerabilities (EPIC, 2018). While TAO have clear espionage and even outright offensive purposes in some situations, the threat of using zero-days as a retaliatory measure in the eventuality of a cyberattack readily contributes to the nation’s cyber deterrent. In this sense, the collection of zero-day vulnerabilities by government agencies such as the NSA can be viewed as increasing the potential for deterrence by threat of retaliation and punishment.

#### Sharing crushes cybersecurity

Benincasa 21 --- Eugenio Benincasa, current WSD-Handa Resident Fellow at Pacific Forum in Honolulu, Hawaii. He holds an MA in International Affairs, “The Case for Cyber ‘Disarmament’ in the European Union”, The International Spectator

Italian Journal of International Affairs

Volume 56, 2021 - Issue 1, https://www.tandfonline.com/doi/pdf/10.1080/03932729.2021.1872200

The focus on the private sector is essential, since the overwhelming majority of network and information systems are privately owned and operated, and most EU member states have not yet adopted the necessary conditions to enable effective vulnerability disclosure by businesses (Pupillo et al. 2018). Nonetheless, as noted previously, government agencies are also actively involved in the search for zero-day vulnerabilities which they can stockpile and use for military purposes. EU member states with known offensive programs include the Netherlands, Sweden, France and Germany (Healey 2016). However, to date, most EU member states have not taken active steps to establish GDDP processes similar to the VEP in the US, and little information is available about how they handle the knowledge of vulnerabilities in their possession (Delcheva and Soesanto 2018). According to Marietje Schaake, former Chair of the CEPS Task Force, “we know that [European] intelligence agencies have been stockpiling vulnerabilities […]. At the moment there’s often a lack of oversight […] intelligence agencies can roughly decide for themselves [whether or not to disclose a newly discovered vulnerability] without proper accountability” (Marietjeschaake.eu 2018). Yet, due to an inherent conflict of interests, as demonstrated by the role of the NSA in the US, these circumstances can hardly lead to optimal results. The absence of a vulnerability review process runs the risk of exposing unpatched vulnerabilities to adversary countries and criminal groups, weakening regional cybersecurity.

### Disclosure Links

#### Over-disclosure of vulnerabilities weakens offensive cyber capabilities

Cushing 14 --- Seychelle Cushing, B.A., Simon Fraser University, 2011, Project Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Arts in the Department of Political Science, SIMON FRASER UNIVERSITY, “Leveraging Information as Power: America’s Pursuit of Cyber Security”, Fall 2014, <http://summit.sfu.ca/system/files/iritems1/14703/etd8726_SCushing.pdf> (accessed via wayback machine)

Nuclear or conventional weapons, once developed, can remain dormant yet functional until needed. In comparison, the zero-days used in cyber weapons require the US to constantly discover new vulnerabilities to maintain a deployable cyber arsenal. Holding a specific zero-day does not guarantee that the vulnerability will remain unpatched for a prolonged period of time by the targeted state.59 Complicating this is the fact that undetected vulnerabilities, once acquired, are rarely used immediately given the time and resources it takes to construct a cyber attack.60 In the time between acquisition and use, a patch for the vulnerability may be released, whether through routine patches or a specific identification of a security hole, rendering the vulnerability obsolete. To minimize this, America deploys several zero-days at once in a cyber attack to increase the odds that at least one (or more) of the vulnerabilities remains open to provide system access.6 2.4.

One Attack, Multiple Vulnerabilities

Multiple backdoor entry points are preferable given that America cannot be absolutely certain of what vulnerabilities the target system will contain62 despite extensive pre-launch cyber attack testing63 and customization.64 A successful cyber attack needs a minimum of one undetected vulnerability to gain access to the target system. Each successive zero-day that works adds to the strength and sophistication of a cyber assault.65 As one vulnerability is patched, America can still rely on the other undetected vulnerabilities to continue its cyber strike. Incorporating multiple undetected vulnerabilities into a cyber attack reduces the need to create new cyber attacks after each zero-day fails.

Stuxnet, a joint US-Israel operation, was a cyber attack designed to disrupt Iran’s progress on its nuclear weapons program.66 The attack was designed to alter the code of Natanz’s computers and industrial control systems to induce “chronic fatigue,” rather than destruction, of the nuclear centrifuges.67 The precision of Stuxnet ensured that all other control systems were ignored except for those regulating the centrifuges.68

What is notable about Stuxnet is its use of four zero-day exploits (of which one was allegedly purchased)69 in the attack.70 That is, to target one system, Stuxnet entered through four different backdoors. A target state aware of a specific vulnerability in its system will enact a patch upon detection and likely assume that the problem is fixed. Exploiting multiple vulnerabilities creates variations in how the attack is executed given that different backdoors alter how the attack enters the target system.71 One patch does not stop the cyber attack. The use of multiple zero-days thus capitalizes on a state’s limited awareness of the vulnerabilities in its system.

Each phase of Stuxnet was different from its previous phase which created confusion among the Iranians. Launched in 2009, Stuxnet was not discovered by the Iranians until 2010.72 Yet even upon the initial discovery of the attack, who the attacker was remained unclear. The failures in the Natanz centrifuges were first attributed to insider error73 and later to China74 before finally discovering the true culprits.75 The use of multiple undetected vulnerabilities helped to obscure the US and Israel as the actual attackers.76

The Stuxnet case helps illustrate the efficacy of zero-day attacks as a means of attaining political goals. Although Stuxnet did not produce immediate results in terminating Iran’s nuclear program, it helped buy time for the Americans to consider other options against Iran. A nuclear Iran would not only threaten American security but possibly open a third conflict for America77 in the Middle East given Israel’s proclivity to strike a nuclear Iran first. Stuxnet allowed the United States to delay Iran’s nuclear program without resorting to kinetic action.78

#### Disclosure allows vendors to patch up vulnerabilities --- this weakens innovation and the discovery of new vulnerabilities

Cushing 14 --- Seychelle Cushing, B.A., Simon Fraser University, 2011, Project Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Arts in the Department of Political Science, SIMON FRASER UNIVERSITY, “Leveraging Information as Power: America’s Pursuit of Cyber Security”, Fall 2014, <http://summit.sfu.ca/system/files/iritems1/14703/etd8726_SCushing.pdf> (accessed via wayback machine)

Cyber defence is an initially disadvantaged position167 given that cyber barriers cannot stop all attacks from penetrating its systems. The ability to absorb a cyber attack, while inconvenient, helps America identify holes in its own security. Although America may be aware of a number of vulnerabilities, additional unaccounted for vulnerabilities will always exist in its systems. A cyber strike thus helps the United States identify where additional previously unknown vulnerabilities exist and, as a result, the US can direct its security apparatus to develop counter-capabilities.

The United States, through the Department of Homeland Security, has launched both passive and active cyber sensors to detect network intrusions. EINSTEIN 2, the passive sensor, was launched in 2008 to detect network intrusions.168 Building on the capabilities of EINSTEIN 2 was EINSTEIN 3, an active sensor designed to provide realtime threat detection capable of stopping known malware before it reaches the targeted government network.169 Passive defences “scan, firewall, and patch” in an attempt to protect a system. These defences, however, have little utility against sophisticated cyber attacks, such as Stuxnet, or against attacks employing zero-days. Active defences, in comparison, build on passive defences to try and stop the cyber attack170 but the success rates of such measures in the US security architecture remains unknown.171 In reality, the EINSTEIN systems only detect and (in the case of EINSTEIN 3) stop known malware entering through known vulnerabilities.172 Nevertheless, every vulnerability subsequently discovered through attack absorption allows EINSTEIN 3 to erect new cyber barriers in its systems.

A cyber-capable adversary may undertake multiple attempts to create sustained access to a target system or network.173 Absorbing the initial attack becomes necessary to find and fix the exploited vulnerability to avert subsequent strikes. If only the first intrusion succeeds, the attacker will be forced to adjust its strike strategy to reopen the system access it once had. By erecting cyber obstacles, one is able to discourage weaker actors from exploiting the same vulnerability before it is patched. Adapting from vulnerabilities to defensive barriers may not stop cyber attacks altogether but it can frustrate cyber-capable states from “easily succeeding in […subsequent] attacks.”174

Allowing a cyber attack, while counterintuitive, allows the US to gather valuable information on its attacker. By identifying how an attacker got into an American system or network and what information was sought, the US is positioned to better understand not only its vulnerabilities but also the capabilities and intentions of its adversaries. Resiliency through attack absorption diminishes the prospect of long-term disruption to American networks. As a result, the benefits to an attacker diminish.175 What was an initial disadvantage can be converted into a long-term security gain.

#### Secrecy is key to effective cyber deterrence and response

John Mowchan 11, Lt Col, October, “Don’t Draw the (Red) Line,” http://www.usni.org/magazines/proceedings/2011-10/dont-draw-red-line

Those arguing for establishing red lines fail to comprehend the complexity of the digital domain, in which adaptation and anonymity are the norm. The United States is better served in the long run by not establishing such thresholds, for four reasons. First, not doing so allows government leaders the latitude to tailor response options based on a hostile act, its physical and digital effects, and how it relates to the current state of affairs in the international system. As retired Air Force General Kevin Chilton remarked in 2009 as commander, U.S. Strategic Command, “I don’t think you take anything off the table when you provide [response] options to the president to decide. Why would we constrain ourselves on how we would respond [to hostile acts in cyberspace]?” 15 Such an approach does not differ from the way the United States addresses hostile acts in other domains. If red lines are established, we will be compelled to respond to each threat that crosses the line, which is unrealistic, given that our computer networks are subjected to millions of probes, scans, and attacks on a daily basis. Even if red lines are narrowly focused (e.g., employing military force if a cyber attack results in the deaths of U.S. citizens), the first time the United States fails to respond accordingly, it will undermine the credibility and deterrence effect of our other capabilities. A second reason in favor of ambiguity is that if our adversaries know our response to such acts, they will adjust accordingly. Because neither the national nor the defense strategy explicitly defines a hostile act in cyberspace or exactly how the United States will respond, this leaves it open to interpretation. As one military official remarked, “If you shut down our power grid, maybe we will put a missile down one of your smokestacks.” 16 In addition, hostile actors may perceive a green light for certain acts that do not cross a particular response threshold. While one such act below this threshold may not be harmful to U.S. interests, what if 100 million are? Again, maintaining ambiguity concerning when, how, and to what extent to respond gives the United States greater latitude. Third, because cyberspace is a global domain that emphasizes open access, the free flow of information, and anonymity, it is extremely difficult to determine where the threat or attack originated. For example, U.S. military networks are probed more than six million times a day by assailants operating in one corner of the world using computer networks or servers in another corner. Most perpetrators are never identified, except for a computer Internet protocol address or a one-time user alias. Army General Keith Alexander, commander of U.S. Cyber Command and Director, National Security Agency, emphasized this challenge, saying, “Too often, the military discovers through forensics that network probes have been successful [and] as a consequence, response becomes policing up after the fact versus mitigating it real time.” 17 If red lines demand a timely response and there is no one to pin responsibility on, then how can a response be implemented? Finally, even if the source of the attacks is determined in a timely manner, automatic triggers for a response, particularly those that employ military force, could create negative second- and third-order effects that make a bad situation even worse. Given that nation states pose the greatest threat to U.S. networks, red lines that automatically result in a response could escalate an already volatile situation. For example, in 2009 individuals in China and Russia penetrated computer networks operating parts of the U.S. electrical power grid. 18 They reportedly inserted malware that could destroy infrastructure components. Although their identities or associations with the Russian and Chinese governments were not disclosed, it validates the point that response options must be tailored. If Russia or China, two nuclear powers, were responsible, a U.S. response would be markedly different than if they had they been conducted by a non-nuclear state. Clearly the diplomatic, information, and economic instruments of national power versus military force would receive more emphasis with China or Russia for what could be considered a hostile act in cyberspace. Given the complex and indeterminate 21st century international system and the multitude of current threats, U.S. interests will be better served by not establishing clear thresholds. Ambiguity is a powerful tool to shape our adversaries’ actions in all domains and allows us the maneuverability to respond where, when, and how we choose. Red-line advocates must understand that thresholds only constrain our actions and could undermine credibility and the power to effectively deter our adversaries.

### Internal Link --- Zero-Days K2 Deterrence

#### Zero-days are key to effective cyber-war offensive capabilities

Gjelten 13 --- Gjelten, Tom. TOM GJELTEN is a correspondent for NPR. Over the years, he has reported extensively from Europe and Latin America, including Cuba. He was reporting live from the Pentagon when it was attacked on September 11, 2001. Subsequently, he covered the war in Afghanistan and Iraq invasion as NPR's lead Pentagon correspondent. Gjelten also covered the first Gulf War and the wars in Croatia and Bosnia, Nicaragua, El Salvador, Guatemala, and Colombia. From Berlin (1990–1994), he covered Europe’s political and economic transition after the fall of the Berlin Wall. Gjelten’s series From Marx to Markets, documenting Eastern Europe’s transition to a market economy, earned him an Overseas Press Club award for the the Best Business or Economic Reporting in Radio or TV. His reporting from Bosnia earned him a second Overseas Press Club Award, a George Polk Award, and a Robert F Kennedy Journalism Award. Gjelten’s books include Sarajevo Daily: A City and Its Newspaper Under Siege, which the New York Times called “a chilling portrayal of a city’s slow murder.” His 2008 book, Bacardi and the Long Fight for Cuba: The Biography of a Cause, was selected as a New York Times Notable Nonfiction Book. "First Strike: US Cyber Warriors Seize the Offensive," World Affairs Journal. January/February 2013. http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive

That was then. Much of the cyber talk around the Pentagon these days is about offensive operations. It is no longer enough for cyber troops to be deployed along network perimeters, desperately trying to block the constant attempts by adversaries to penetrate front lines. The US military’s geek warriors are now prepared to go on the attack, armed with potent cyberweapons that can break into enemy computers with pinpoint precision. The new emphasis is evident in a program launched in October 2012 by the Defense Advanced Research Projects Agency (DARPA), the Pentagon’s experimental research arm. DARPA funding enabled the invention of the Internet, stealth aircraft, GPS, and voice-recognition software, and the new program, dubbed Plan X, is equally ambitious. DARPA managers said the Plan X goal was “to create revolutionary technologies for understanding, planning, and managing cyberwarfare.” The US Air Force was also signaling its readiness to go into cyber attack mode, announcing in August that it was looking for ideas on how “to destroy, deny, degrade, disrupt, deceive, corrupt, or usurp the adversaries [sic] ability to use the cyberspace domain for his advantage.” The new interest in attacking enemies rather than simply defending against them has even spread to the business community. Like their military counterparts, cybersecurity experts in the private sector have become increasingly frustrated by their inability to stop intruders from penetrating critical computer networks to steal valuable data or even sabotage network operations. The new idea is to pursue the perpetrators back into their own networks. “We’re following a failed security strategy in cyber,” says Steven Chabinsky, formerly the head of the FBI’s cyber intelligence section and now chief risk officer at CrowdStrike, a startup company that promotes aggressive action against its clients’ cyber adversaries. “There’s no way that we are going to win the cybersecurity effort on defense. We have to go on offense.” The growing interest in offensive operations is bringing changes in the cybersecurity industry. Expertise in patching security flaws in one’s own computer network is out; expertise in finding those flaws in the other guy’s network is in. Among the “hot jobs” listed on the career page at the National Security Agency are openings for computer scientists who specialize in “vulnerability discovery.” Demand is growing in both government and industry circles for technologists with the skills to develop ever more sophisticated cyber tools, including malicious software—malware—with such destructive potential as to qualify as cyberweapons when implanted in an enemy’s network. “Offense is the biggest growth sector in the cyber industry right now,” says Jeffrey Carr, a cybersecurity analyst and author of Inside Cyber Warfare. But have we given sufficient thought to what we are doing? Offensive operations in the cyber domain raise a host of legal, ethical, and political issues, and governments, courts, and business groups have barely begun to consider them. The move to offensive operations in cyberspace was actually under way even as Pentagon officials were still insisting their strategy was defensive. We just didn’t know it. The big revelation came in June 2012, when New York Times reporter David Sanger reported that the United States and Israel were behind the development of the Stuxnet worm, which had been used to damage computer systems controlling Iran’s nuclear enrichment facilities. Sanger, citing members of President Obama’s national security team, said the attacks were code-named Olympic Games and constituted “America’s first sustained use of cyberweapons.” The highly sophisticated Stuxnet worm delivered computer instructions that caused some Iranian centrifuges to spin uncontrollably and self-destruct. According to Sanger, the secret cyber attacks had begun during the presidency of George W. Bush but were accelerated on the orders of Obama. The publication of such a highly classified operation provoked a firestorm of controversy, but government officials who took part in discussions of Stuxnet have not denied the accuracy of Sanger’s reporting. “He nailed it,” one participant told me. In the aftermath of the Stuxnet revelations, discussions about cyber war became more realistic and less theoretical. Here was a cyberweapon that had been designed and used for the same purpose and with the same effect as a kinetic weapon: like a missile or a bomb, it caused physical destruction. Security experts had been warning that a US adversary could use a cyberweapon to destroy power plants, water treatment facilities, or other critical infrastructure assets here in the United States, but the Stuxnet story showed how the American military itself could use an offensive cyberweapon against an enemy. The advantages of such a strike were obvious. A cyberweapon could take down computer networks and even destroy physical equipment without the civilian casualties that a bombing mission would entail. Used preemptively, it could keep a conflict from evolving in a more lethal direction. The targeted country would have a hard time determining where the cyber attack came from. In fact, the news that the United States had actually developed and used an offensive cyberweapon gave new significance to hints US officials had quietly dropped on previous occasions about the enticing potential of such tools. In remarks at the Brookings Institution in April 2009, for example, the then Air Force chief of staff, General Norton Schwartz, suggested that cyberweapons could be used to attack an enemy’s air defense system. “Traditionally,” Schwartz said, “we take down integrated air defenses via kinetic means. But if it were possible to interrupt radar systems or surface to air missile systems via cyber, that would be another very powerful tool in the tool kit allowing us to accomplish air missions.” He added, “We will develop that—have [that]—capability.” A full two years before the Pentagon rolled out its “defensive” cyber strategy, Schwartz was clearly suggesting an offensive application. The Pentagon’s reluctance in 2011 to be more transparent about its interest in offensive cyber capabilities may simply have reflected sensitivity to an ongoing dispute within the Obama administration. Howard Schmidt, the White House Cybersecurity Coordinator at the time the Department of Defense strategy was released, was steadfastly opposed to any use of the term “cyber war” and had no patience for those who seemed eager to get into such a conflict. But his was a losing battle. Pentagon planners had already classified cyberspace officially as a fifth “domain” of warfare, alongside land, air, sea, and space. As the 2011 cyber strategy noted, that designation “allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests.” That statement by itself contradicted any notion that the Pentagon’s interest in cyber was mainly defensive. Once the US military accepts the challenge to fight in a new domain, it aims for superiority in that domain over all its rivals, in both offensive and defensive realms. Cyber is no exception. The US Air Force budget request for 2013 included $4 billion in proposed spending to achieve “cyberspace superiority,” according to Air Force Secretary Michael Donley. It is hard to imagine the US military settling for any less, given the importance of electronic assets in its capabilities. Even small unit commanders go into combat equipped with laptops and video links. “We’re no longer just hurling mass and energy at our opponents in warfare,” says John Arquilla, professor of defense analysis at the Naval Postgraduate School. “Now we’re using information, and the more you have, the less of the older kind of weapons you need.” Access to data networks has given warfighters a huge advantage in intelligence, communication, and coordination. But their dependence on those networks also creates vulnerabilities, particularly when engaged with an enemy that has cyber capabilities of his own. “Our adversaries are probing every possible entry point into the network, looking for that one possible weak spot,” said General William Shelton, head of the Air Force Space Command, speaking at a CyberFutures Conference in 2012. “If we don’t do this right, these new data links could become one of those spots.” Achieving “cyber superiority” in a twenty-first-century battle space is analogous to the establishment of air superiority in a traditional bombing campaign. Before strike missions begin against a set of targets, air commanders want to be sure the enemy’s air defense system has been suppressed. Radar sites, antiaircraft missile batteries, enemy aircraft, and command-and-control facilities need to be destroyed before other targets are hit. Similarly, when an information-dependent combat operation is planned against an opposing military, the operational commanders may first want to attack the enemy’s computer systems to defeat his ability to penetrate and disrupt the US military’s information and communication networks. Indeed, operations like this have already been carried out. A former ground commander in Afghanistan, Marine Lieutenant General Richard Mills, has acknowledged using cyber attacks against his opponent while directing international forces in southwest Afghanistan in 2010. “I was able to use my cyber operations against my adversary with great impact,” Mills said, in comments before a military conference in August 2012. “I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations.” Mills was describing offensive cyber actions. This is cyber war, waged on a relatively small scale and at the tactical level, but cyber war nonetheless. And, as DARPA’s Plan X reveals, the US military is currently engaged in much larger scale cyber war planning. DARPA managers want contractors to come up with ideas for mapping the digital battlefield so that commanders could know where and how an enemy has arrayed his computer networks, much as they are now able to map the location of enemy tanks, ships, and aircraft. Such visualizations would enable cyber war commanders to identify the computer targets they want to destroy and then assess the “battle damage” afterwards. Plan X would also support the development of new cyber war architecture. The DARPA managers envision operating systems and platforms with “mission scripts” built in, so that a cyber attack, once initiated, can proceed on its own in a manner “similar to the auto-pilot function in modern aircraft.” None of this technology exists yet, but neither did the Internet or GPS when DARPA researchers first dreamed of it. As with those innovations, the government role is to fund and facilitate, but much of the experimental and research work would be done in the private sector. A computer worm with a destructive code like the one Stuxnet carried can probably be designed only with state sponsorship, in a research lab with resources like those at the NSA. But private contractors are in a position to provide many of the tools needed for offensive cyber activity, including the software bugs that can be exploited to provide a “back door” into a computer’s operating system. Ideally, the security flaw or vulnerability that can be exploited for this purpose will be one of which the network operator is totally unaware. Some hackers specialize in finding these vulnerabilities, and as the interest in offensive cyber operations has grown, so has the demand for their services. The world-famous hacker conference known as Defcon attracts a wide and interesting assortment of people each year to Las Vegas: creative but often antisocial hackers who identify themselves only by their screen names, hackers who have gone legit as computer security experts, law enforcement types, government spies, and a few curious academics and journalists. One can learn what’s hot in the hacker world just by hanging out there. In August 2012, several attendees were seated in the Defcon cafe when a heavy-set young man in jeans, a t-shirt, and a scraggly beard strolled casually up and dropped several homemade calling cards on the table. He then moved to the next table and tossed down a few more, all without saying a word. There was no company logo or brand name on the card, just this message: “Paying top dollar for 0-day and offensive technologies . . . ” The card identified the buyer as “zer0daybroker” and listed an e-mail address. A “zero-day” is the most valuable of computer vulnerabilities, one unknown to anyone but the researcher who finds it. Hackers prize zero-days because no one knows to have prepared a defense against them. The growing demand for these tools has given rise to brokers like Zer0day, who identified himself in a subsequent e-mail exchange as “Zer0 Day Haxor” but provided no other identifying information. As a broker, he probably did not intend to hack into a computer network himself but only to act as an intermediary, connecting sellers who have discovered system vulnerabilities with buyers who want to make use of the tools and are willing to pay a high price for them. In the past, the main market for these vulnerabilities was software firms themselves who wanted to know about flaws in their products so that they could write patches to fix them. Big companies like Google and Microsoft employ “penetration testers” whose job it is to find and report vulnerabilities that would allow someone to hack into their systems. In some cases, such companies have paid a bounty to freelance cyber researchers who discover a vulnerability and alert the company engineers. But the rise in offensive cyber operations has transformed the vulnerability market, and hackers these days are more inclined to sell zero-days to the highest bidder. In most cases, these are governments. The market for back-door exploits has been boosted in large part by the burgeoning demand from militaries eager to develop their cyber warfighting capabilities. The designers of the Stuxnet code cleared a path into Iranian computers through the use of four or five separate zero-day vulnerabilities, an achievement that impressed security researchers around the world. The next Stuxnet would require the use of additional vulnerabilities. “If the president asks the US military to launch a cyber operation in Iran tomorrow, it’s not the time to start looking for exploits,” says Christopher Soghoian, a Washington-based cybersecurity researcher. “They need to have the exploits ready to go. And you may not know what kind of computer your target uses until you get there. You need a whole arsenal [of vulnerabilities] ready to go in order to cover every possible configuration you may meet.” Not surprisingly, the National Security Agency—buying through defense contractors—may well be the biggest customer in the vulnerability market, largely because it pays handsomely. The US military’s dominant presence in the market means that other possible purchasers cannot match the military’s price. “Instead of telling Google or Mozilla about a flaw and getting a bounty for two thousand dollars, researchers will sell it to a defense contractor like Raytheon or SAIC and get a hundred thousand for it,” says Soghoian, now the principal technologist in the Speech, Privacy and Technology Project at the American Civil Liberties Union and a prominent critic of the zero-day market. “Those companies will then turn around and sell the vulnerability upstream to the NSA or another defense agency. They will outbid Google every time.”

### Internal Link --- China Invades Taiwan

#### Losing our comparative advantage emboldens China to take Taiwan – that breaks down cyber deterrence and turns heg

Hjortdal 11 --- Magnus Hjortdal is a researcher associated with CHINA-SEC, Centre for Military Studies at the University of Copenhagen, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." Journal of Strategic Security 4, no. 2 (2011) : 1-24. DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1 Available at: https://digitalcommons.usf.edu/jss/vol4/iss2/2

China's military strategy mentions cyber capabilities as an area that the People's Liberation Army (PLA) should invest in and use [on a large scale](https://muhaz.org/back-to-pre-history-v3.html). 13 The U.S. Secretary of Defense, Robert Gates, has also declared that China's development in the cyber area increasingly concerns him, 14 and that there has been a decade-long trend of cyber attacks emanating from China. 15

Virtually all digital and electronic military systems can be attacked via cyberspace. Therefore, it is essential for a state to develop capabilities in this area if it wishes to challenge the present American hegemony. The interesting question then is whether China is developing capabilities in cyberspace in order to deter the United States. 16

<Table Omitted>

China's military strategists describe cyber capabilities as a powerful asymmetric opportunity in a deterrence strategy. 19 Analysts consider that an "important theme in [Chinese writings on computer](https://muhaz.org/years-56-chinese-program-second-year--semester-one.html)-network operations (CNO) is the use of computer-network attack (CNA) as the spearpoint of deterrence." 20 CNA increases the enemy's costs to become too great to engage in warfare in the first place, which Chinese analysts judge to be essential for deterrence. 21 This could, for example, leave China with the potential ability to deter the United States from intervening in a scenario concerning Taiwan. CNO is viewed as a focal point for the People's Liberation Army, but it is not clear how the actual capacity functions or precisely what condit ions it works under. 22

If a state with superpower potential (here China) is to create an opportunity to ascend militarily and politically in the international system, it would require an asymmetric [deterrence capability](https://muhaz.org/simulation-games-michael-maurer.html) such as that described here. 23 It is said that the "most significant computer network attack is characterized as a pre-emption weapon to be used under the rubric of the rising Chinese strategy of [...] gaining mastery before the enemy has struck." 24 Therefore, China, like other states seeking a similar capacity, has recruited massively within the hacker milieu inside China. 25 Increasing resources in the PLA are being allocated to develop assets in relation to cyberspace. 26 The improvements are visible: The PLA has established " information warfare " capabilities, 27 with a special focus on cyber warfare that, [according to their doctrine](https://muhaz.org/lars-puvogel-i-introduction.html), can be used in peacetime. 28 Strategists from the PLA advocate the use of virus and hacker attacks that can paralyze and surp rise its enemies. 29

#### Successful China cyberattack key to a first strike

Jennings 21 --- Ralph Jennings, Voice of America, “How China Could Cyberattack Taiwan”, December 10, 2021, https://www.voanews.com/a/how-china-could-cyberattack-taiwan/6349594.html

Disable first, strike later?

China could disable Taiwanese computer systems that run transport, utilities and defense operations to make a military strike easier, scholars suggest.

“If there is a war, and the Chinese shut down the power grid through a cyberattack, that may not completely shut down Taiwan’s defense system, but it’s going to have an impact,” Sun said.

Successful cyberattacks on financial institutions and other targets would shake people’s confidence, said Alexander Huang, chairman of a military strategy research foundation in Taipei. All of Taiwan’s “critical infrastructure” is connected by the internet, he added, a linkage that could cause “great difficulties” as well as widespread panic among people.

“If we got a cyberwar, then all these systems are down,” Huang said. “If the communication node is broken, then it would be a form of decapitation.”

Advanced conventional weapons such as new submarines and aircraft would be of little use during a debilitating cyberattack, he said, adding that it’s unclear whether Taiwan’s government has taken enough measures to guard against a major cyberattack.

### Internal Link --- China Cyberstrikes US

#### Cyber capabilities are key to deterrence and defending against China

Gompert and Libicki 15 --- Gompert, David C. and Libicki, Martin. David C. Gompert is the Principle Deputy Director of National Intelligence. He is a Senior Fellow at RAND and a Distinguished Visiting Professor at the National Defense University's Center for Technology and National Security Policy. Gompert received his BA in Engineering from the US Naval Academy and his MPA from Princeton University. Martin Libicki received his PhD in Economics from UC Berkeley, his MA in City and Regional Planning from UC Berkeley, and his BSc in Mathematics from MIT. He is a Professor at the RAND Graduate School and a Senior Management Scientist at RAND. “Waging Cyber War the American Way,” Survival: Global Politics and Strategy. August–September 2015. Vol 57., 4th ed, pp 7-28. 07-22-2015. http://www.iiss.org/en/publications/survival/sections/2015-1e95/survival--global-politics-and-strategy-august-september-2015-c6ba/57-4-02-gompert-and-libicki-eab1

At the same time, the United States regards cyber war during armed conflict with a cyber-capable enemy as probable, if not inevitable. It both assumes that the computer systems on which its own forces rely to deploy, receive support and strike will be attacked, and intends to attack the computer systems that enable opposing forces to operate as well. Thus, the United States has said that it can and would conduct cyber war to ‘support operational and contingency plans’ – a euphemism for attacking computer systems that enable enemy war fighting. US military doctrine now regards ‘non-kinetic’ (that is, cyber) measures as an integral aspect of US joint offensive operations.8 Even so, the stated purposes of the US military regarding cyber war stress protecting the ability of conventional military forces to function as they should, as well as avoiding and preventing escalation, especially to non-military targets. Apart from its preparedness to conduct counter-military cyber operations during wartime, the United States has been reticent about using its offensive capabilities. While it has not excluded conducting cyber operations to coerce hostile states or non-state actors, it has yet to brandish such a threat.9 Broadly speaking, US policy is to rely on the threat of retaliation to deter a form of warfare it is keen to avoid. Chinese criticism that the US retaliatory policy and capabilities ‘will up the ante on the Internet arms race’ is disingenuous in that China has been energetic in forming and using capabilities for cyber operations.10 Chinese criticism is disingenuous Notwithstanding the defensive bias in US attitudes toward cyber war, the dual missions of deterrence and preparedness for offensive operations during an armed conflict warrant maintaining superb, if not superior, offensive capabilities. Moreover, the case can be made – and we have made it – that the United States should have superiority in offensive capabilities in order to control escalation.11 The combination of significant capabilities and declared reluctance to wage cyber war raises a question that is not answered by any US official public statements: when it comes to offence, what are US missions, desired effects, target sets and restraints – in short, what is US policy? To be clear, we do not take issue with the basic US stance of being at once wary and capable of cyber war. Nor do we think that the United States should advertise exactly when and how it would conduct offensive cyber war. However, the very fact that the United States maintains options for offensive operations implies the need for some articulation of policy. After all, the United States was broadly averse to the use of nuclear weapons during the Cold War, yet it elaborated a declaratory policy governing such use to inform adversaries, friends and world opinion, as well as to forge domestic consensus. Indeed, if the United States wants to discourage and limit cyber war internationally, while keeping its options open, it must offer an example. For that matter, the American people deserve to know what national policy on cyber war is, lest they assume it is purely defensive – or just too esoteric to comprehend. Whether to set a normative example, warn potential adversaries or foster national consensus, US policy on waging cyber war should be coherent. At the same time, it must encompass three distinguishable offensive missions: wartime counter-military operations, which the United States intends to conduct; retaliatory missions, which the US must have the will and ability to conduct for reasons of deterrence; and coercive missions against hostile states, which could substitute for armed attack.12 Four cases serve to highlight the relevant issues and to inform the elaboration of an overall policy to guide US conduct of offensive cyber war. The first involves wartime counter-military cyber operations against a cyber-capable opponent, which may also be waging cyber war; the second involves retaliation against a cyber-capable opponent for attacking US systems other than counter-military ones; the third involves coercion of a ‘cyber-weak’ opponent with little or no means to retaliate against US cyber attack; and the fourth involves coercion of a ‘cyber-strong’ opponent with substantial means to retaliate against US cyber attack. Of these, the first and fourth imply a willingness to initiate cyber war. Counter-military cyber war during wartime Just as cyber war is war, armed hostilities will presumably include cyber war if the belligerents are both capable of and vulnerable to it. The reason for such certainty is that impairing opposing military forces’ use of computer systems is operationally compelling. Forces with requisite technologies and skills benefit enormously from data communications and computation for command and control, intelligence, surveillance and reconnaissance (ISR), targeting, navigation, weapon guidance, battle assessment and logistics management, among other key functions. If the performance of forces is dramatically enhanced by such systems, it follows that degrading them can provide important military advantages. Moreover, allowing an enemy to use cyber war without reciprocating could mean military defeat. Thus, the United States and other advanced states are acquiring capabilities not only to use and protect computer systems, but also to disrupt those used by enemies. The intention to wage cyber war is now prevalent in Chinese planning for war with the United States – and vice versa. Chinese military planners have long made known their belief that, because computer systems are essential for effective US military operations, they must be targeted. Chinese cyber capabilities may not (yet) pose a threat to US command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) networks, which are well partitioned and protected. However, the networks that enable logistical support for US forces are inviting targets. Meant to disable US military operations, Chinese use of cyber war during an armed conflict would not be contingent on US cyber operations. Indeed, it could come early, first or even as a precursor of armed hostilities. For its part, the US military is increasingly aware not only that sophisticated adversaries like China can be expected to use cyber war to degrade the performance of US forces, but also that US forces must integrate cyber war into their capabilities and operations. Being more dependent on computer networks to enhance military performance than are its adversaries, including China, US forces have more to lose than to gain from the outbreak of cyber war during an armed conflict. This being so, would it make sense for the United States to wait and see if the enemy resorts to cyber war before doing so itself? Given US conventional military superiority, it can be assumed that any adversary that can use cyber war against US forces will do so. Moreover, waiting for the other side to launch a cyber attack could be disadvantageous insofar as US forces would be the first to suffer degraded performance. Thus, rather than waiting, there will be pressure for the United States to commence cyber attacks early, and perhaps first. Moreover, leading US military officers have strongly implied that cyber war would have a role in attacking enemy anti-access and area-denial (A2AD) capabilities irrespective of the enemy’s use of cyber war.13 If the United States is prepared to conduct offensive cyber operations against a highly advanced opponent such as China, it stands to reason that it would do likewise against lesser opponents. In sum, offensive cyber war is becoming part and parcel of the US war-fighting doctrine. The nature of US counter-military cyber attacks during wartime should derive from the mission of gaining, or denying the opponent, operational advantage. Primary targets of the United States should mirror those of a cyber-capable adversary: ISR, command and control, navigation and guidance, transport and logistics support. Because this mission is not coercive or strategic in nature, economic and other civilian networks should not be targeted. However, to the extent that networks that enable military operations may be multipurpose, avoidance of non-military harm cannot be assured. There are no sharp ‘firebreaks’ in cyber war.14

#### China would initiate preemptive cyber strikes on the US

Freedberg 13 --- Freedberg, Sydney J. Sydney J. Freedberg Jr. is the deputy editor for Breaking Defense. He graduated summa cum laude from Harvard with an AB in History and holds an MA in Security Studies from Georgetown University and a MPhil in European Studies from Cambridge University. During his 13 years at National Journal magazine, he wrote his first story about what became known as "homeland security" in 1998, his first story about "military transformation" in 1999, and his first story on "asymmetrical warfare" in 2000. Since 2004 he has conducted in-depth interviews with more than 200 veterans of Afghanistan and Iraq about their experiences, insights, and lessons-learned, writing stories that won awards from the association of Military Reporters & Editors in 2008 and 2009, as well as an honorable mention in 2010. "China’s Fear Of US May Tempt Them To Preempt: Sinologists," Breaking Defense. 10-1-2013. http://breakingdefense.com/2013/10/chinas-fear-of-us-may-tempt-them-to-preempt-sinologists/2

WASHINGTON: Because China believes it is much weaker than the United States, they are more likely to launch a massive preemptive strike in a crisis. Here’s the other bad news: The current US concept for high-tech warfare, known as Air-Sea Battle, might escalate the conflict even further towards a “limited” nuclear war, says one of the top American experts on the Chinese military. [This is one in an occasional series on the crucial strategic relationship and the military capabilities of the US, its allies and China.] What US analysts call an “anti-access/area denial” strategy is what China calls “counter-intervention” and “active defense,” and the Chinese approach is born of a deep sense of vulnerability that dates back 200 years, China analyst Larry Wortzel said at the Institute of World Politics: “The People’s Liberation Army still sees themselves as an inferior force to the American military, and that’s who they think their most likely enemy is.” That’s fine as long as it deters China from attacking its neighbors. But if deterrence fails, the Chinese are likely to go big or go home. Chinese military history from the Korean War in 1950 to the Chinese invasion of Vietnam in 1979 to more recent, albeit vigorous but non-violent, grabs for the disputed Scarborough Shoal suggests a preference for a sudden use of overwhelming force at a crucial point, what Clausewitz would call the enemy’s “center of gravity.” “What they do is very heavily built on preemption,” Wortzel said. “The problem with the striking the enemy’s center of gravity is, for the United States, they see it as being in Japan, Hawaii, and the West Coast….That’s very escalatory.” (Students of the American military will nod sagely, of course, as we remind everyone that President George Bush made preemption a centerpiece of American strategy after the terror attacks of 2001.) Wortzel argued that the current version of US Air-Sea Battle concept is also likely to lead to escalation. “China’s dependent on these ballistic missiles and anti-ship missiles and satellite links,” he said. Since those are almost all land-based, any attack on them “involves striking the Chinese mainland, which is pretty escalatory.” “You don’t know how they’re going to react,” he said. “They do have nuclear missiles. They actually think we’re more allergic to nuclear missiles landing on our soil than they are on their soil. They think they can withstand a limited nuclear attack, or even a big nuclear attack, and retaliate.” What War Would Look Like So how would China’s preemptive attack unfold? First would come weeks of escalating rhetoric and cyberattacks. There’s no evidence the Chinese favor a “bolt out of the blue” without giving the adversary what they believe is a chance to back down, agreed retired Rear Adm. Michael McDevitt and Dennis Blasko, former Army defense attache in Beijing, speaking on a recent Wilson Center panel on Chinese strategy where they agreed on almost nothing else. That’s not much comfort, though, considering that Imperial Japan showed clear signs they might attack and still caught the US flat-footed at Pearl Harbor. When the blow does fall, the experts believe it would be sudden. Stuxnet-style viruses, electronic jamming, and Israeli-designed Harpy radar-seeking cruise missiles (similar to the American HARM but slower and longer-ranged) would try to blind every land-based and shipborne radar. Long-range anti-aircraft missiles like the Russian-built S-300 would go for every plane currently in the air within 125 miles of China’s coast, a radius that covers all of Taiwan and some of Japan. Salvos of ballistic missiles would strike every airfield within 1,250 miles. That’s enough range to hit the four US airbases in Japan and South Korea – which are, after all, static targets you can look up on Google Maps – to destroy aircraft on the ground, crater the runways, and scatter the airfield with unexploded cluster bomblets to defeat repair attempts. Long-range cruise missiles launched from shore, ships, and submarines then go after naval vessels. And if the Chinese get really good and really lucky, they just might get a solid enough fix on a US Navy aircraft carrier to lob a precision-guided ballistic missile at it. But would this work? Maybe. “This is fundamentally terra incognita,” Heritage Foundation research fellow Dean Cheng told me. There has been no direct conventional clash between major powers since Korea in the 1950s, no large-scale use of anti-ship missiles since the Falklands in 1982, and no war ever where both sides possessed today’s space, cyber, electronic warfare, and precision-guided missile capabilities. Perhaps the least obvious but most critical uncertainty in a Pacific war would be invisible. “I don’t think we’ve seen electronic warfare on a scale that we’d see in a US-China confrontation,” said Cheng. “I doubt very much they are behind us when it comes to electronic warfare, [and] the Chinese are training every day on cyber: all those pings, all those attacks, all those attempts to penetrate.” While the US has invested heavily in jamming and spoofing over the last decade, much of the focus has been on how to disable insurgents’ roadside bombs, not on how to counter a high-tech nation-state. China, however, has focused its electronic warfare and cyber attack efforts on the United States. Conceptually, China may well be ahead of us in linking the two. (F-35 supporters may well disagree with this conclusion.) Traditional radar jammers, for example, can also be used to insert viruses into the highly computerized AESA radars (active electronically scanned array) that are increasingly common in the US military. “Where there has been a fundamental difference, and perhaps the Chinese are better than we are at this, is the Chinese seem to have kept cyber and electronic warfare as a single integrated thing,” Cheng said. “We are only now coming round to the idea that electronic warfare is linked to computer network operations.” In a battle for the electromagnetic spectrum, Cheng said, the worst case “is that you thought your jammers, your sensors, everything was working great, and the next thing you know missiles are penetrating [your defenses], planes are being shot out of the sky.”

### A2: China Won’t Risk It

#### Yes risk, they are ramping up military pressure, and Xi has control of the party decision making and lacks checks, if Xi can deliver on his promise for Chinese glory he will take it

Bas van Beurden. Bas van Beurden is a student enrolled in the Master’s program International Relations & Diplomacy at Leiden University in cooperation with the Clingendael Institute in the Netherlands.This article is part of a special issue on Taiwan-US relations under Biden presidency for the Taiwan studies programme, The Taiwan Studies Programme is a research centre based at the University of Nottingham focusing on all aspects of contemporary Taiwan. The Taiwan Studies Programme does not privilege political positions and the views published on Taiwan Insight are those of the author and not the institute., 12-3-2020, Deterrence & Dialogue: How Washington Can Prevent a US-China War Over Taiwan," Taiwan Insight, https://taiwaninsight.org/2020/12/03/deterrence-dialogue-how-washington-can-prevent-a-us-china-war-over-taiwan/, Accessed: 1-17-2021, MB

Can the United States and China escape Thucydides Trap? While international relations experts grapple with the question whether the two powers are destined for war, a storm seems to be gathering in the Asia-Pacific, and it seems increasingly clear where lightning might strike. Considering recent developments, the Taiwan Straits seems to be the most likely battleground for Sino-American conflict. The prospect of conflict appears to be looming as Beijing closes in on Hong Kong and ratchets up its rhetoric on a forceful reunification with Taiwan.

China has backed its statements on “the Chinese dream of national rejuvenation” with a substantial increase in military activity surrounding Taiwan. It has conducted an unprecedented amount of more than ten military and transit exercises in close proximity to Taiwan in 2020. Additionally, China’s air force made an incursion into Taiwanese airspace for the first time in 20 years. Since then, it has done so an accumulative number of times. A former top military official of Taiwan commented that Beijing might be looking to provoke a military reaction by Taipei, which could give them a casus belli for an invasion.

Weakness is Provocative

These developments come as Taiwan’s defence and resolve have withered, which has been exacerbated by the Sino-American military balance of power having shifted in favour of China. Taiwan has grown complacent under the security umbrella. It scrapped its mandatory conscription in 2018, and its overall defence strategy of late makes little military sense. Instead of focussing its limited defence budget on creating an effective defence force tailored towards Chinese offensive capabilities, it has concentrated on trying to match China in more traditional and expensive weapon systems; such as tanks, fighter jets, and submarines. At the same time, Washington does not seem to be capable of ensuring Taiwan’s defence. Senior US Defence officials have revealed that the US would no longer win in a war against China; especially not one over the defence of Taiwan.

Such a development is particularly concerning due to the centralisation of Chinese decision-making. China, under Xi Jinping, has noticeably become more assertive and less risk-averse. Xi reportedly seems to be making important decisions himself. An erosion of checks and balances is worrying since it could easier lead to undaunted actions regarding a forceful reunification with Taiwan. This concern is compounded by Beijing possibly being encouraged by an increasingly isolationist US. After all, Russia met relatively little resistance when it invaded Georgia and Ukraine. A Beijing insider informed reporter Evan Osnos that Xi had told people that he was impressed by Putin’s annexation of Crimea. Meanwhile, Xi might also be emboldened by his own endeavours, as a result of the marginal resistance China met in regards to its tightening control over Hong Kong. China’s ambitious and unconstrained leader might figure that today’s strategic conditions are as ripe as will probably ever be for the remainder of his leadership. Thus, he might seize the opportunity to personally restore China’s former glory by forcefully reuniting with Taiwan sooner rather than later.

### Terminal --- China / Taiwan

#### Taiwan goes nuclear

Lowther 13 – William Lowther, Taipei Times, citing a report by the Center for Strategic and International Studies, 3/16/13, “Taiwan could spark nuclear war: report,” <http://www.taipeitimes.com/News/taiwan/archives/2013/03/16/2003557211>

Taiwan is the most likely potential crisis that could trigger a nuclear war between China and the US, a new academic report concludes.¶ “Taiwan remains the single most plausible and dangerous source of tension and conflict between the US and China,” says the 42-page report by the Washington-based Center for Strategic and International Studies (CSIS).¶ Prepared by the CSIS’ Project on Nuclear Issues and resulting from a year-long study, the report emphasizes that Beijing continues to be set on a policy to prevent Taiwan’s independence, while at the same time the US maintains the capability to come to Taiwan’s defense.¶ “Although tensions across the Taiwan Strait have subsided since both Taipei and Beijing embraced a policy of engagement in 2008, the situation remains combustible, complicated by rapidly diverging cross-strait military capabilities and persistent political disagreements,” the report says.¶ In a footnote, it quotes senior fellow at the US Council on Foreign Relations Richard Betts describing Taiwan as “the main potential flashpoint for the US in East Asia.”¶ The report also quotes Betts as saying that neither Beijing nor Washington can fully control developments that might ignite a Taiwan crisis.¶ “This is a classic recipe for surprise, miscalculation and uncontrolled escalation,” Betts wrote in a separate study of his own.¶ The CSIS study says: “For the foreseeable future Taiwan is the contingency in which nuclear weapons would most likely become a major factor, because the fate of the island is intertwined both with the legitimacy of the Chinese Communist Party and the reliability of US defense commitments in the Asia-Pacific region.”¶ Titled Nuclear Weapons and US-China Relations, the study says disputes in the East and South China seas appear unlikely to lead to major conflict between China and the US, but they do “provide kindling” for potential conflict between the two nations because the disputes implicate a number of important regional interests, including the interests of treaty allies of the US.¶ The danger posed by flashpoints such as Taiwan, the Korean Peninsula and maritime demarcation disputes is magnified by the potential for mistakes, the study says.¶ “Although Beijing and Washington have agreed to a range of crisis management mechanisms, such as the Military Maritime Consultative Agreement and the establishment of a direct hotline between the Pentagon and the Ministry of Defense, the bases for miscommunication and misunderstanding remain and draw on deep historical reservoirs of suspicion,” the report says.¶ For example, it says, it is unclear whether either side understands what kinds of actions would result in a military or even nuclear response by the other party.¶ To make things worse, “neither side seems to believe the other’s declared policies and intentions, suggesting that escalation management, already a very uncertain endeavor, could be especially difficult in any conflict,” it says.¶ Although conflict “mercifully” seems unlikely at this point, the report concludes that “it cannot be ruled out and may become increasingly likely if we are unwise or unlucky.”¶ The report says: “With both sides possessing and looking set to retain formidable nuclear weapons arsenals, such a conflict would be tremendously dangerous and quite possibly devastating.”

#### Global nuclear war

**Hunkovic 9** (Lee J, American Military University, “The Chinese-Taiwanese Conflict: Possible Futures of a Confrontation between China, Taiwan and the United States of America”, [http://www.lamp-method.org/eCommons/ Hunkovic.pdf](http://www.lamp-method.org/eCommons/Hunkovic.pdf))

A war between China, Taiwan and the United States has the potential to escalate into a nuclear conflict and a third world war, therefore, many countries other than the primary actors could be affected by such a conflict, including Japan, both Koreas, Russia, Australia, India and Great Britain, if they were drawn into the war, as well as all other countries in the world that participate in the global economy, in which the United States and China are the two most dominant members. If China were able to successfully annex Taiwan, the possibility exists that they could then plan to attack Japan and begin a policy of aggressive expansionism in East and Southeast Asia, as well as the Pacific and even into India, which could in turn create an international standoff and deployment of military forces to contain the threat. In any case, if China and the United States engage in a full-scale conflict, there are few countries in the world that will not be economically and/or militarily affected by it. However, China, Taiwan and United States are the primary actors in this scenario, whose actions will determine its eventual outcome, therefore, other countries will not be considered in this study.

#### China/Taiwan war goes nuclear

**Glaser 11**

(Charles, Professor of Political Science and International Affairs at the Elliott School of International Affairs at George Washington University, Director of the Institute for Security and Conflict Studies, “Will China’s Rise lead to War? ,” Foreign Affairs March/April 2011, <http://web.clas.ufl.edu/users/zselden/coursereading2011/Glaser.pdf>)

THE PROSPECTS for avoiding intense military competition and war may be good, but growth in China's power may nevertheless require some changes in U.S. foreign policy that Washington will find disagreeable--particularly regarding Taiwan. Although it lost control of Taiwan during the Chinese Civil War more than six decades ago, China still considers Taiwan to be part of its homeland, and unification remains a key political goal for Beijing. China has made clear that it will use force if Taiwan declares independence, and much of China's conventional military buildup has been dedicated to increasing its ability to coerce Taiwan and reducing the United States' ability to intervene. Because China places such high value on Taiwan and because the United States and China--whatever they might formally agree to--have such different attitudes regarding the legitimacy of the status quo, the issue poses special dangers and challenges for the U.S.-Chinese relationship, placing it in a different category than Japan or South Korea. A crisis over Taiwan could fairly easily escalate to nuclear war, because each step along the way might well seem rational to the actors involved. Current U.S. policy is designed to reduce the probability that Taiwan will declare independence and to make clear that the United States will not come to Taiwan's aid if it does. Nevertheless, the United States would find itself under pressure to protect Taiwan against any sort of attack, no matter how it originated. Given the different interests and perceptions of the various parties and the limited control Washington has over Taipei's behavior, a crisis could unfold in which the United States found itself following events rather than leading them. Such dangers have been around for decades, but ongoing improvements in China's military capabilities may make Beijing more willing to escalate a Taiwan crisis. In addition to its improved conventional capabilities, China is modernizing its nuclear forces to increase their ability to survive and retaliate following a large-scale U.S. attack. Standard deterrence theory holds that Washington's current ability to destroy most or all of China's nuclear force enhances its bargaining position. China's nuclear modernization might remove that check on Chinese action, leading Beijing to behave more boldly in future crises than it has in past ones. A U.S. attempt to preserve its ability to defend Taiwan, meanwhile, could fuel a conventional and nuclear arms race. Enhancements to U.S. offensive targeting capabilities and strategic ballistic missile defenses might be interpreted by China as a signal of malign U.S. motives, leading to further Chinese military efforts and a general poisoning of U.S.-Chinese relations.

### A2: “Won’t Invade/Will Be Lower Level”

#### Even lower scale coercive measures escalate

Michael E. O’Hanlon 19. Senior fellow at The Brookings Institution, specializing in defense and foreign policy issues. He co-directs the Security and Strategy team, the Defense Industrial Base working group, and the Africa Security Initiative within the Foreign Policy program. Adjunct professor at Columbia, Georgetown, and Syracuse universities, and a member of the International Institute for Strategic Studies. 4-30-2019. "The Senkaku Paradox: Risking Great Power War Over Small Stakes." Brookings Institution Press. Chapter 2. pg. 43-50. JSTOR. accessed 10-23-2019//JDi

A possible Chinese blockade of Taiwan, on the other hand, clearly has even higher stakes, and history suggests that crises may again occur in connection with Taiwan. Beijing might convince itself that a blockade-centered operation against Taiwan, designed to force it to reverse whatever purportedly offending action or rhetoric had caused China’s reaction in the first place, might not be hugely risky. In principle, China could scale back or suspend enforcement of the blockade at any point if it needed to, and could do so while saving face, especially if the blockade was conducted principally by submarines. Moreover, Beijing might believe that even a partially effective naval blockade could be a potent instrument of coercion against Taiwan. Such a blockade would almost assuredly be nowhere near complete or airtight.84 However, China would not need to stop all commercial ships transiting into and out of Taiwan. It would simply need to deter enough ships from risking the journey that Taiwan’s economy would suffer badly. The goal would likely be to squeeze the island economically to the point of capitulation. This solution might seem quite elegant from Beijing’s point of view: it could involve little or no loss of life, little or no damage to Taiwan itself, and the ability to back off the attack if the United States seemed prepared to intervene or if the world community slapped major trade sanctions on China in response.85 In any such blockade, China might well combine various elements of military power, including cyberattacks, into a multidimensional operation.86 It could attack command and control as well as reconnaissance capabilities both on land and in space (the latter intended largely to blind the United States). The centerpiece of the approach would probably be the PRC submarine fleet introducing a significant risk factor into all maritime voyages into and out of Taiwan by occasionally sinking a cargo ship, either with submarines or with mines it had laid in Taiwan’s harbors.87 The PRC submarine force has improved by leaps and bounds in recent decades. Over the past twenty years, China’s fleet of modern attack subs has grown from roughly two to forty.88 China’s precision-strike capabilities have improved to the point that China could conceivably use a preemptive missile and air attack against Taiwanese airfields and ports and associated infrastructure to hobble Taiwan’s ability to strike back, though it might choose not to attack Taiwan’s territory in the first instance.89 To allow humanitarian supplies to reach Taiwan, Beijing might offer countries the option of first docking in a PRC port for inspection before sailing to their destinations. In this and other ways, it could limit the dangers to innocent civilians. Since this strategy might require the Chinese submarine fleet to sink only a few ships to achieve the desired aims, even in the worst case Beijing might believe that it was acting humanely— threatening the lives of only 100 to 200 commercial seamen. Given the perceived stakes involved, Beijing could well consider this a reasonable risk. If they chose to try to break the blockade, the basic concept of operations for the United States and Taiwan would probably be to assemble enough forces in the western Pacific to set up a protected shipping lane east of Taiwan. To carry out that mission, the United States would need to establish air superiority throughout a large part of the region, together with Taiwan (and perhaps other countries such as Japan). The United States and Taiwan, and perhaps others, would also need to protect ships against Chinese submarine attack while coping with the threat of mines near Taiwan’s ports. And they might have to do all this without assured access to much of their satellite architecture, especially for imagery and some types of signals intelligence. That is because China’s abilities to shoot down or disable low Earth orbit satellites, through direct-ascent interceptors or directed-energy weapons or other means, have improved in recent years (even as some aspects of U.S. access to space have become more distributed and resilient as well).90 China might well be willing to shoot at American satellites even if it sought, at least initially, not to attack U.S. ships or aircraft. However, its willingness to do the latter in addition should not be dismissed, in light of Taiwan’s importance to Beijing. And its willingness would likely grow very quickly after the first Chinese submarine was sunk, which could happen if the U.S.-Taiwan blockade-busting and convoy escort operation shot back at a PLA submarine that had just attacked a cargo vessel. Escalation could happen fast. Later in a conflict, China might even consider using nuclear weapons in such an attack, despite its official no-first-use policy, as Columbia professor Thomas Christensen has argued.91 While the term “surgical nuclear strike” is almost oxymoronic and Strangelovian, to the extent it has any faint resemblance to reality, it is probably in a situation like an attack on a lone ship at sea. Establishing air superiority has become much harder for the United States and Japan in these kinds of scenarios because of the PLA Air Force’s modernization trends in recent years, combined with the limited options for basing U.S. aircraft in the region. Fortunately, modern U.S. stealthy or “fifth-generation” aircraft are still far superior to Chinese planes. Unfortunately, China now has close to 1,000 “fourth-generation” fighters roughly comparable to U.S. aircraft such as the F-15 and F-16. And it can base perhaps 1,000 aircraft within several hundred miles of Taiwan. A RAND simulation estimates that China might be able to surge about half that number in an attack on Taiwan or on the shipping around it, including a mix of air-to-air, air-to-ground, and electronic-warfare planes. Using a basic model and some simplifying assumptions, RAND estimates that the United States could prevent such a surge force from reaching most of its targets only by continuously keeping some two wings or about 150 aircraft airborne near Taiwan. The United States and its partners would likely succeed in such an effort because, according to RAND’s model, the United States’ fifthgeneration aircraft—F-22s and F-35s, and to a lesser degree F/A-18E/F Super Hornets—could have 50 percent more lethality and up to 90 percent less vulnerability than Chinese combat jets.92 But the success would come at a price, and only with considerable effort and difficulty. China could choose the time and place of its surge, and the United States (with any allies) would therefore have to be vigilant at all times. It would need to keep fighters airborne near Taiwan essentially for as long as the crisis endured. It would also need the continued presence of airborne warning aircraft in the vicinity. Bases on Okinawa are about 750 kilometers away from Taiwan, or about an hour of flight time; aircraft carriers might be kept roughly that close too. But other bases in the area—Misawa Air Base on Japan’s main Honshu island, Andersen Air Force base on Guam— would be 2,500 kilometers or more distant, meaning some three hours of flying each way to get to station and then return after flying a patrol. If aircraft and crews are limited to a daily flight average of about six hours a day, jets from Okinawa could average 1.5 sorties per day and those from the more distant bases slightly less than one sortie per twenty-four hours. That would translate into three hours a day on station flying from Kadena and 1.5 hours a day flying from Guam or Honshu. Put differently: Eight aircraft (plus or minus) based on Kadena would be needed to sustain one on station near Taiwan. Sixteen aircraft or so based at Misawa or Andersen Air Force Base would be needed to keep one on station near Taiwan. Averaging this out, keeping two wings of fighters aloft at a time could require about ten to twelve times that number being based in the region, or twenty to twenty-four wings—more than half the total U.S. military aggregate. (The RAND study actually estimates that fourteen to thirty would be needed, depending on specific assumptions; I have simplified the analysis above.93) Moreover, the United States could lose a number of aircraft in this process, perhaps even dozens. China could lose dozens or even hundreds. The backdrop would be set for escalation. Both sides would be increasingly tempted to attack the land bases and aircraft carriers from which planes operated.94 Ballistic missiles and ballistic missile defense would be important in this kind of engagement, too. China now has missiles, such as the medium-range DF-21 in the Dong-Feng series, that are capable of being fired from its homeland and reaching ships east of Taiwan. It is not clear whether the United States could blind China’s sensors adequately to deprive the PLA of targeting information. Any PLA attack against military facilities in a place like Okinawa therefore could well shut down runways for at least some stretch of time and destroy aircraft or ordnance and fuel stocks not in underground areas or hardened shelters.95 Again, Chinese nuclear attacks against American and any allied naval assets in the region are hard to dismiss categorically. The antisubmarine warfare (ASW) effort could have multiple aspects. The United States would probably be tempted to deploy its own attack submarines as close as possible to China—certainly in the Taiwan Strait, maybe just outside PRC ports. This approach would provide American submarines a good prospect of destroying PRC submarines at their source, before they were in position to fire on commercial shipping (or U.S. aircraft carriers) in more distant waters. However, this type of ASW could be escalatory if it involved attacks in Chinese territorial waters. Whatever happened near Chinese shores, there would surely be additional layers of American ASW farther out to sea. American ASW assets on ships and planes would accompany convoys of merchant ships as they sailed in from the open ocean waters east of Taiwan. These convoys might form a thousand miles or more east of Taiwan and enjoy armed protection from that point onward as they traveled to the island, and then later as they departed. The ASW assets would use sonar to listen for submarines, and for the sound of any torpedoes being fired. The United States would have to deploy significant numbers of surface combatants and airplanes such as P-3s and P-8s, as well as helicopters, to the region for this mission. Some would help protect U.S. aircraft carriers east of Taiwan. Others would provide additional protection to merchant ships or mine warfare vessels as they operated near Taiwan’s shores. Any Chinese submarine wishing to fire a torpedo at a merchant ship or aircraft carrier would then first have to run a gauntlet (if it were firing long-range antiship missiles, it could avoid some of the gauntlet, but would depend on targeting information provided by another platform). It would likely have to evade submarine detection as it left port, avoid any openwater search missions that the United States and Taiwan established, and then somehow penetrate the defensive ASW perimeter of whatever convoy it was attacking as it approached its target. To survive the overall engagement and return to port, it would then need to successfully negotiate all of this in the other direction. Unfortunately for Chinese submarines, this would be risky business. Unfortunately for the United States, Taiwan, and any other allies participating in the effort, it would also be risky for their assets, and some would surely be lost in the operation. During the Cold War, the effectiveness of ASW operations was commonly assessed at 5 to 15 percent per barrier. (Cold War barriers were often more linear and literal perimeters than would be likely here, but the fact remains that Chinese submarines would have to survive perhaps three types of pursuers on three different parts of their journey to or from home base.) By those odds, the typical Chinese submarine would do well to survive for two or three round-trip missions from base.96 But it might succeed in getting off several shots against valuable, and vulnerable, surface ships before meeting its own demise.97 A recent major RAND study on the U.S.-China military balance concurred with this broad result, especially in cases where Chinese submarines could be cued by sensors to a general area where a target such as a U.S. aircraft carrier might operate. In that case, a given submarine might have multiple opportunities to get off shots at lucrative surface targets.98 China might hope that a quick strike that sank a major U.S. ship and killed hundreds of Americans (or even thousands, in the event of a carrier sinking) would cause Washington to waver in its future commitment to the defense of Taiwan. The United States might face serious challenges in waters near Taiwan as well, despite the proximity of land-based assets that could join in the ASW hunt. Shallow waters are complex sonar environments in which sound waves bounce back and forth in multiple and unpredictable directions. This makes ambush a real worry, especially for the mine warfare vessels and surface ships that would have to escort commercial vessels all the way into Taiwan’s ports.99 Toward a Net Assessment Where does this leave us? Although I have not provided a detailed scenario analysis or combat modeling exercise here, the broad contours of the situation drive home some central points. They are also consistent with the more detailed modeling work of others, such as RAND. Once a Chinese blockade operation against Taiwan began, it would be difficult to be confident that it would end without a significant and escalating conflict pitting the United States, Taiwan, and perhaps Japan against China. If that occurred, sustained naval, aerial, and missile combat in and around Taiwan would likely lead to substantial losses on all sides. American advantages in fifth-generation combat aircraft and modern attack submarines would give the United States and its partners in the operation a significant edge. However, that edge is less than it used to be. China would clearly have the edge in geography, and it also increasingly possesses good attack submarines and precision-strike missiles as well. Myriad uncertainties, including the survivability of space and cyber systems, as well as ships and land bases, make it hard to be confident in predicting outcomes. Indeed, when I modeled uncertainties with respect to a possible U.S.- led invasion of Iraq in 2002, I produced a likely band of possible casualties in which higher estimates were literally ten times greater than lower estimates. This broad approach was eventually vindicated: it initially appeared, in April 2003, that U.S. losses might be very modest, but over the course of several years it became clear they were much higher. A U.S.- China war would be far more uncertain. For most scenarios involving blockades and other possible intense operations over and in the waters of the western Pacific, the United States and allies could probably muscle their way to victory over China at this point, as we approach 2020. Taiwan could also likely endure the privations that would be experienced during the military campaign before victory was assured.100 My best guess is that both sides would lose most low-altitude satellites and some cyber as well as command, control, and communications capability, so the war would ultimately be fought in a certain fog. Yet American high-tech advantages in weapons platforms would ultimately provide an important and probably decisive edge. This somewhat sanguine conclusion is far from certain, however. It hinges in part on a willingness in Washington to accept many thousands of American battlefield dead and at least some risk of nuclear escalation. Even though U.S. nuclear forces far exceed those of the PLA, China might conclude that its disproportionate interests in the Taiwan issue warranted nuclear brinkmanship, especially if China had already possibly lost thousands of its own people in conventional combat, which would heighten the stakes as well as the reputational importance of the outcome of the conflict. These concerns could be amplified if the United States, intentionally or not, began to strike the nuclear assets of the PLA in the course of conventional fighting near Taiwan. If that happened, China might face a “use them or lose them” dilemma.101 Nuclear attack against a carrier, or a high-altitude nuclear airburst over a base like Kadena (designed to destroy people and equipment immediately below, without generating lots of fallout), might seem particularly attractive options to Beijing. Nuclear escalation might happen in another way as well. Perhaps China would attempt a large-scale cyberattack against the United States (and quite possibly Japan too) in the course of such a conflict. Its hope might be, for example, to incapacitate the U.S. electricity grid—as National Security Agency director Admiral Michael Rogers said in 2014 that China might well be able to do. Such a result could badly incapacitate many of the Defense Department systems in the United States that require civilianproduced electricity to function.102 Even if such systems could be restored quickly, the U.S. electrical system as a whole might remain damaged for many months, as might national infrastructure needed to deploy military forces abroad. Whether the United States could muster a major military response at a time when its national capacities were needed to take care of the many Americans left in the cold and dark, without medicine or sanitation or clean water or viable living quarters, is an open question. China might hope that U.S. military assets would be devoted to missions closer to home, to prevent mass famine, privation, or disease, after such a catastrophe. China might do this, if already losing in a conventional conflict or expecting to lose, even if its own cyber systems could be just as vulnerable to attack.103 Countries sometimes start wars or escalate not out of complete confidence that they will succeed but after concluding that the risks of inaction outweigh those of even risky action.104 And if China conducted such a cyber operation, it might be the very type of non-nuclear strategic attack that the Trump administration’s Nuclear Posture Review envisions as a plausible basis for possible American nuclear first use.105

### China Revisionism

#### China’s revisionist—Official statements prove. Prefer official statements because empirics can be evaluated multiple ways, only statements provide a clear demonstration of resolve.

#### Three framing issues:

#### a. Even if they aren’t revisionist now, they’re hiding their true intentions until they have the capabilities to challenge the US, plan gives them that golden opportunity—that’s a basic tenant of realism.

b. To win China is not revisionist they have to explain every action as defensive. Revisionism does not preclude defensive actions, but defensive realism precludes any offensive actions.

#### **c.** Only a risk we get offense—if China is revisionist, deterrence is the only option because they pocket concessions. But, even if they’re defensive, deterrence can’t hurt because it sends a signal that they can’t win.

#### Yes revisionism:

#### A. Territory

Dean Cheng and Carson 18 (Dean Cheng, Senior Research Fellow, Asian Studies Center, Davis Institute for National Security and Foreign Policy, at the Heritage Foundation. He specializes in China’s military and foreign policy, in particular China’s relationship with its Asian neighbors and with the United States. He’s being interviewed on the Jaw-Jaw podcast by Brad Carson is a professor at the University of Virginia, where he teaches in the Batten School of Leadership and Public Policy. 11-13-2018, "Jaw-Jaw: China is a Funny Sort of Revisionist Power — A Conversation with Dean Cheng," War on the Rocks, https://warontherocks.com/2018/11/jaw-jaw-china-is-a-funny-sort-of-revisionist-power-a-conversation-with-dean-cheng/, Accessed: 7-27-2019 /Kent Denver-YBJL)

If you look at the South China Sea and the so-called Nine-Dash Line, the Chinese are very upfront, often in stating. Vietnam? It doesn’t get an exclusive economic zone. It barely gets territorial waters three miles off of its shores. Never mind 12 or 24. Same for the Philippines. They are now pushing Indonesia, which even 10 years ago, the Chinese said, “Well, you know no Indonesian territory falls within our claims.” Now, they’re like, “Oh, no. Indonesia’s exclusive economic zone needs to be truncated,” because of China’s claims. International waterways that transit through the South China Sea carry 5.3 trillion dollars of trade. We are talking the carotid artery of global trade, and the Chinese are saying, “That’s my artery.”

#### B. Internet censorship

Dean Cheng and Carson 18 (Dean Cheng, Senior Research Fellow, Asian Studies Center, Davis Institute for National Security and Foreign Policy, at the Heritage Foundation. He specializes in China’s military and foreign policy, in particular China’s relationship with its Asian neighbors and with the United States. He’s being interviewed on the Jaw-Jaw podcast by Brad Carson is a professor at the University of Virginia, where he teaches in the Batten School of Leadership and Public Policy. 11-13-2018, "Jaw-Jaw: China is a Funny Sort of Revisionist Power — A Conversation with Dean Cheng," War on the Rocks, https://warontherocks.com/2018/11/jaw-jaw-china-is-a-funny-sort-of-revisionist-power-a-conversation-with-dean-cheng/, Accessed: 7-27-2019 /Kent Denver-YBJL)

When we look at the internet and how China has balkanized the internet, how it is trying to basically affect where and who has access to the internet. Where it is saying, “Only nation states should be really allowed to authorize what is allowed onto the internet.” And by the way, if I, China, don’t like who you’re letting on, you should take measures. Follow the gold, pro-Democratic elements, the New York Times, we have the right to keep you off the internet, or at least outside of China’s piece of the internet. Free flow of information, an absolute bedrock of modern day global economies, would fall by the wayside.

#### C. Space weapons

Dean Cheng and Carson 18 (Dean Cheng, Senior Research Fellow, Asian Studies Center, Davis Institute for National Security and Foreign Policy, at the Heritage Foundation. He specializes in China’s military and foreign policy, in particular China’s relationship with its Asian neighbors and with the United States. He’s being interviewed on the Jaw-Jaw podcast by Brad Carson is a professor at the University of Virginia, where he teaches in the Batten School of Leadership and Public Policy. 11-13-2018, "Jaw-Jaw: China is a Funny Sort of Revisionist Power — A Conversation with Dean Cheng," War on the Rocks, https://warontherocks.com/2018/11/jaw-jaw-china-is-a-funny-sort-of-revisionist-power-a-conversation-with-dean-cheng/, Accessed: 7-27-2019 /Kent Denver-YBJL)

And we’re seeing the Chinese regularly now threatening items in space. The 2007 ASAT test, other tests with lasers, things like that. Development of ASAT capabilities. Again, what is outer space? It is international common space. You can’t draw boundary up 100, 300, 5,000 miles from your border and say, “This is mine.” And yet the Chinese are increasingly making moves to say, “You know you shouldn’t be able to just fly over my country with your satellite.” Never mind orbital mechanics. “And take pictures and eavesdrop, just like you shouldn’t be able to fly aircraft and do other things off my shores.”

#### They are committed to counter extended deterrence, it’s a core of liberal order of alliances

Dean Cheng 2017, Senior Research Fellow The Heritage Foundation 6. Space Deterrence, the U.S.-Japan Alliance, and Asian Security: A U.S. Perspective, In Harold, Scott W., Yoshiaki Nakagawa, Junichi Fukuda, John A. Davis, Keiko Kono, Dean Cheng, and Kazuto Suzuki, The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains. Santa Monica, CA: RAND Corporation, 2017. <https://www.rand.org/pubs/conf_proceedings/CF379.html>.,

A final complication stems from the asymmetric alliance relationships that characterize the United States and China. During the Cold War, both the United States and the Soviet Union had allies and commitments outside their national territories. Consequently, there were at least some parallels in terms of understanding extended deterrence. In the case of China, however, Beijing does not have any real allies that it is clearly and credibly committed to defending. (Although China and North Korea are, at least on paper, linked by their 1961 Mutual Defense Treaty, many observers doubt that this commitment is truly binding on either side.) For Beijing, neither Pakistan nor North Korea, the closest analogues, are really comparable to the U.S. relationship with Japan.

As a result, China does not face the problem of extending deterrence; it is defending itself but it is not attempting to defend allies. Indeed, it would be more accurate to say that China is not focused on engaging in extended deterrence, but on countering extended deterrence. Along its periphery, China does not directly confront the United States; it is seeking to deter and coerce U.S. friends and allies. This creates substantially different asymmetric concerns between China and the United States. Where Washington is engaged in extended deterrence in support of allies, Beijing is concerned about direct deterrence—i.e., direct threats to China.

## Advantage CP

**Advantage CP --- 1NC**

**The North Atlantic Treaty Organization should;**

- re-establishing regular meetings of the NRC at the level of ambassadors

- establish a dialogue on cyber activities within the NRC

- invite experts to brief the NRC on cyberspace regulations

- create a NATO-Russia hotline in case of serious cyber incidents

**CP solves NATO-Russia escalation**

**Kubiak 19** --- Dr Katarzyna Kubiak et al, Policy Fellow on nuclear and arms control policy at the European Leadership Network. Previously, she was a Transatlantic Post-Doc Fellow for International Relations and Security (TAPIR) at the Norwegian Institute for Defence Studies and an associate at the German Institute for International and Security Affairs (SWP), , “Towards a More Stable NATO-Russia Relationship” EURO-ATLANTIC SECURITY REPORT, Feb 2019, https://www.europeanleadershipnetwork.org/wp-content/uploads/2019/02/31012019-Towards-a-more-stable-Russia-NATO-relationship.pdf

There are functioning channels of communication between NATO and Russia, including meetings of the NATO-Russia Council (NRC) at ambassadorial level. But these channels are of limited effectiveness. The intensity of NATO-Russia contacts has been **drastically** reduced following Russia’s actions against Ukraine and NATO’s subsequent April 2014 decision to suspend practical cooperation with Russia. With increased military activities and what each side perceives as pressure or probing of its limits and ‘red lines’ by the other, whether intended or not, the existing communication channels are inadequate and insufficient to clarify concerns or deal with uncertainties, especially during periods of increased tension. The level of mutual understanding between Russia and NATO is **low**, and the deterrence signalling of each side can be misunderstood by the other side or dismissed by them as posturing.

NATO and Russia will have to navigate better a space filled with substantial and genuine disagreements, ballooning mistrust regarding the other side’s intentions, and continued prioritisation of deterrence and strengthening of respective military potentials.

In navigating safely, the priority should thus be given to “deepening” and multiplying the current channels of communication and making the best possible use of the existing instruments such as the NRC or the Organization for Security and Co-operation in Europe (OSCE) and its Structured Dialogue. None of the actions suggested below would breach the ‘red lines’ constraining the conduct of the bilateral relationship, as currently understood by NATO or Russia. They can be also pursued in parallel with efforts to utilise better all other available instruments such as the OSCE-wide and bilateral confidencebuilding measures and the Open Skies Treaty. These proposals **may appear trivial** or modest, but their implementation **would mark an improvement in** comparison with **the current situation,** moving Russia and NATO towards **more stability and predictability**.

Better quality of dialogue While respecting the existing limitations, for example regarding NATO’s de facto decision not to resume working-group level NRC contacts, **the following measures could be pursued**:

• Schedule regular meetings of the NRC at the level of ambassadors

Between 2014 and 2018, ten meetings of the NATO-Russia Council were held. Three took place in both 2016 and 2017 and two in 2018.3 Topics included the situation in and around Ukraine (featured as the fixed first point of the agenda); transparency and risk reduction in the context of military activities, other issues of concern including the situation in Afghanistan, aviation security in the Baltic region, **hybrid challenges** or the Intermediate-Range Nuclear Forces Treaty.

While this may suggest increased efficiency of contacts, the exact timing and agenda has had to be laboriously negotiated each time before the NRC met. The **infrequent** and **adhoc character** of the meetings increases the risk of important concerns not being raised in a timely way or of falling off the agenda. It does not give enough scope to prepare the meetings, ensure proper follow-up, or develop any positive dynamics between them.

**Setting a firm timetable** with a specified number of **regular meetings** (either bimonthly or quarterly, with additional emergency meetings scheduled as needed) would provide **more consistency**, avoid divisive deliberations on the timing, make the channel less vulnerable to political storms and allow more continuity of work.

As Chairman, the NATO Secretary General could take a more leading role in setting the agenda, with NATO’s Deputy Secretary General working with the Russian Permanent Representation to develop the preparatory materials for the meetings.

The first NRC meeting in 2019 took place on 25th January, with the INF Treaty crisis high on its agenda. While there was no progress on resolving the crisis, the meeting illustrated the need to discuss issues of mutual importance in a timely and efficient manner.

• Russia to ensure ambassadorial level representation at the NRC

Since January 2018, there has been no Russian ambassador to NATO.4 Such a long gap without a senior Russian diplomat with a direct connection to Moscow’s decisionmaking circles hinders a constructive dialogue in the NRC and seems to signal Russian disinterest in improving relations with NATO. It may also hamper communication during any period of increased tension.

Russia could immediately appoint a Permanent Representative to NATO to signal the importance of maintaining relations and make sustained engagement possible. Alternatively, Russia could assign one of the two Russian ambassadors currently in Brussels (one responsible for bilateral relations and one for the European Union) to take over responsibility for the NATO portfolio, or appoint a Moscow-based ambassador to participate in the NRC meetings. Even under the NATO limits on the Russian delegation, Russia could also bring in more senior diplomats, military and civilian experts to brief the NRC on topics of mutual interest and to prepare its meetings. The participation of Deputy Foreign Minister Sergei Ryabkov in the January 2019 NRC meeting was a welcome development.

• Ensure that there are multiple channels of military-to-military communication

More military-to-military contacts would add to the stability of the relationship by improving understanding of the other, offering options on channels to be used in a crisis and creating some **trust** at a personal level. Dialogue and technical contacts between the uniformed personnel of Russia and NATO should not be a victim of lack of trust at the political level. So far, there have been **sporadic telephone conversations** and direct meetings between the Chief of the General Staff of the Russian Armed Forces General Valery Gerasimov and NATO’s Supreme Allied Commander Europe (SACEUR) General Curtis Scaparrotti, as well as with previous Chairman of the NATO Military Committee General Petr Pavel.

The new Chairman of the NATO Military Committee Air Chief Marshal Sir Stuart Peach could **re-establish communication** with the Russian Chief of the General Staff, in parallel with the existing SACEUR-Gerasimov channel. Based on a clear political mandate with a clearly understood separation of functions, these contacts could be made **routine** and prepared at deputies’ level. While the SACEUR-Gerasimov channel could focus on the most pressing military activities, operations-related issues and current concerns, the Peach-Gerasimov exchanges could focus on more political and longer-term questions related to military doctrines, postures, development of capabilities and concepts of operations. Improved and multiple contacts would serve as another instrument to clarify concerns, increase transparency and build up mutual understanding and personal trust.

• Use the existing NATO-Russia hotline in case of serious cyber incidents

NATO and Russia **lack** established joint procedures to deal with serious cyberincidents and allegations of cyber-attacks, despite the fact that these can have disastrous consequences and despite the increase in the scale and sophistication of cyber-attacks, sometimes attributed to states. In some cases, particular NATO states and Russia would rather use bilateral instruments to communicate and react, but in case of a major or widespread attacks against military targets, it may be useful to have the possibility to interact at the NATO-Russia level as well.

Due to the technical nature of any conversation about a potential incident, a separate **cyber incidents hotline** between NATO and Russia may be preferable. Since this may not be feasible to set up, the already existing NATO-Russia military-to-military hotline should also be activated in the event of a cyber-contingency. Both NATO and Russia could agree that they would be prepared to use the hotline for that purpose, and that issue-experts would be available to advise the leadership of each side in case of its activation. The use of the Nuclear Risk Reduction Centres in Washington and Moscow to facilitate inquiries about cybersecurity incidents could serve as a blueprint.

While it would not solve the bigger problem of establishing rules and norms in the cyberdomain, the hotline would help to **control the risk of escalation** in the event of a serious cyber-attack against a NATO member state or Russia conducted by a third party or a non-state entity. It could become **crucial** in such cases to **prevent a false attribution** of the attack and retaliation against the wrong target.

More substance to dialogue Increasing the frequency of NATO-Russia meetings or military-to-military contacts would have limited impact unless the two sides look anew at the topics and potential of the conversation. While not requiring any major policy changes, these recommendations would enable both sides to reflect on their goals for NATO-Russia relations:

• **NATO’s homework**: clarify the content of ‘no business as usual’

NATO Allies want to avoid any impression of getting back to what they call “business as usual” with Moscow, in other words resuming cooperation with Russia while putting aside the current disagreements, notably over Ukraine. Without a clearer meaning of the term, however, any activity or topics beyond the current agenda can be presented as crossing the line. At the same time, individual NATO states continue, to varying degrees, to pursue bilateral contacts with Russia on topics of mutual interest. That may with time create a gap between limited exchanges at the NATO-Russia level and closer engagement at national level in some cases. It may therefore be in NATO’s interest to review its approach to dialogue. The North Atlantic Council could clarify through internal discussion what NATO understands by “no business as usual” and “no practical cooperation” with Russia.

While clearly delineating areas of no engagement (for example, no cooperation on sensitive issues like missile defence or joint exercises), that could open up space and give an impetus for **business that needs to be done**. This could include increased political and military-to-military contacts, risk reduction measures, arrangements for crisis prevention and management, and engagement in confidence-building and arms control talks with Russia.

• Russia’s homework: address the credibility gap in its dialogue offers towards NATO

While Russia maintains that it makes attempts to pragmatically engage the Alliance and its members, including on crisis management, and is open to resumption of working-level contacts, it has a serious credibility problem. Many Allies see Moscow as not engaging seriously on some issues (such as specific questions on military exercises or military build-up), cherry-picking topics or making proposals calculated to divide the Alliance rather than to be constructive. NATO also frequently claims that Russia’s actions on the ground are inconsistent with its engagement initiatives.

Russian decision-makers are certainly entitled to conclude that dialogue with NATO is pointless. But if they are going to engage in dialogue at all, and especially if they are interested in stabilising the relationship with NATO and addressing the threat of escalation, they will need to reflect on the effectiveness of their overall approach towards NATO and its member states. A review could ensure that diplomatic overtures are not unintentionally undermined by assertive propaganda or military moves on the ground. Regarding specific topics, Moscow could provide credible information on its military activities at the NRC briefings and constructively address more of the questions raised by the NATO side.

• Run a Table Top Exercise on the Management of Air Incidents

Significant steps have already been taken to reduce risks of collision between military and civilian aircraft (for example, through the Baltic Sea Project Team and the International Civil Aviation Organization), but more should be done in the military-to-military sphere where dangerous incidents continue to be an issue.5 While so far escalation has been avoided, real-time management of an incident or accident involving the air forces of NATO countries and Russia would prove to be challenging, as the November 2015 Turkey-Russia incident demonstrated.

A table top exercise focused on air accident/ incident response could develop a much needed procedural knowledge for handling such situations. A non-governmental panel of experts could be convened from both sides (including retired senior military with the requisite expertise, as well as civil aviation experts) to scope the problem, run a table top exercise with scenarios involving reacting to an air incident or accident, and prepare recommendations. Such a panel could report to the NRC, with results made available to the OSCE and other interested organisations. This exercise could provide a blueprint for perfecting procedures (such as the preparation of a code of conduct) that could be discussed at the governmental level in order to improve the handling of air incidents.

• Invite experts to brief the NRC on cyberspace regulations

The scope for advancing NATO-Russia discussion on crisis stability by acting “from within” the NRC seems limited. This is particularly true for the cyber domain, where the NRC conversation so far has apparently been unproductive. At the same time, the need for greater regulation of cyberspace activities is growing more acute, and a number of international initiatives have been launched to work on solutions. To move forward the discussions related to the cyber domain within the NRC, it may be beneficial to draw on the experience of external experts such as members of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security6 or the Global Commission on the Stability of Cyberspace (GCSC).7

When it comes to air safety, the briefing by the Baltic Sea Project Team helped the NRC to better comprehend the topic. Similarly, independent cyberspace experts could brief the NRC on their work and lessons-learned, making recommendations relevant to the NRC which could be further discussed by the Council.

Intensifying NATO-Russia dialogue beyond the official government level contacts

There are contacts between individual experts, think tanks and academic experts from Russia and NATO countries, as well as sporadic joint initiatives. Yet deterioration of the relationship has increased the tendency to instrumentalise expert discussions as opportunities for trading accusations rather than for engaging in a constructive dialogue. This seems to consolidate rather than help to overcome the existing diplomatic stalemate.

Non-governmental initiatives and those with the informal participation of officials do not always require official blessing or implicate governmental positions yet can provide valuable insights and suggestions for intergovernmental work. They can operate at a more technical level, outside the political limelight.

Initiatives to consider could include setting up a “Track 2 NATO-Russia Council” of NGOs, think tanks and scientific organisations; establishing a group of retired officials and experts to advise the officials on both sides, or setting up a Wise Persons Study Panel to offer recommendations on the future of the NATO-Russia relationship. Additionally, the NATO Parliamentary Assembly’s Bureau could maintain contacts with the Russian Parliament in order to cultivate dialogue and explore the potential of ad-hoc meetings.

Significant value-added can be derived from joint simulations (table top exercises, war games or scenario-based discussions) involving experts, former officials and retired military from NATO states, partners and Russia. For example, simulations with the participation of retired officials and officers could “test” responses to a developing crisis between NATO and Russia, examine escalation scenarios and crisis management procedures. Such exercises could help assess the dangers of inadvertent escalation, the likelihood or otherwise of a rapid move to a devastating conflict, and the adequacy of the current communication arrangements. A potential post-INF Treaty escalation of tensions in Europe caused by deployments of INF Treaty-class missiles could serve as one possible scenario.

On another track, taking the Polish-Russian project “White Spots―Black Spots: Difficult Matters in Polish-Russian Relations” as a point of departure, a semi-official study of the history of NATO-Russian relations could be initiated. The participation of historians from NATO countries and Russia, with a broad access to archives, could help to analyse the roots of some misunderstandings and myths about the past, or at least illuminate better the conflicting narratives and historical perspectives.

III Taking one step further in stabilising NATO-Russia relations

The limited character of the recommendations in the previous section stems from a realistic assessment of what is feasible in the current circumstances. NATO's and Russia's approaches to their relationship are based on deeply-held views about the other side and their own interests. It is difficult to see how the present confrontational relationship can be significantly improved unless its trajectory is changed by internal developments or external events.

The simplest but also least likely scenario for improvement would be a major reconceptualisation of the relationship on either side. From NATO's perspective, the change on Russia's side would most likely need to include reversing the policy decisions of recent years including the annexation of Crimea, restraint in its force deployments and exercises, ceasing Russia's destabilisation campaign, accepting NATO as a partner rather than a threat, reversing Moscow's negative stance on NATO's enlargement and addressing the numerous issues brought up by the Allies. From Russia’s perspective, such a change would probably have to involve NATO accepting Russia’s recent territorial gains, significantly restraining its military activities along its Eastern flank, and accepting a halt on Eastern enlargement and limitations on partnerships with countries bordering Russia. It is implausible to expect either side to make such a dramatic U-turn.

It may thus be more realistic to envisage increased stabilisation of the relationship as stemming from a gradual build-up of greater predictability between NATO and Russia. Implementation of the recommendations from the previous section would be one step in that direction. Parallel progress on resolving some of the contentious issues, such as the implementation of the Minsk Agreements, the situation in the Azov Sea, or the INF Treaty, would be another. A partial “détente” would mean a slow, careful and reversible broadening of the areas of engagement, dealing with some of the sharpest points of difference and avoidance of new tensions.

If and when political space opens up that makes such increased engagement possible, maintaining movement would require both sides to respond step-by-step to the opportunity. That supports the case for having ‘in the air’ ideas that have already to some extent been sifted. These might range from additional channels of communication, potential political pledges, declaratory measures, or crisis management procedures, to initiating limited cooperation on issues of mutual interest.

Our exercise identified a short menu of ideas that did not meet the requirement of immediate political feasibility but that were nonetheless seen as **practical and realistic** enough that they might become applicable at a certain point. If they were implemented, NATO-Russia relations would still be adversarial but would **be much more stable** and somewhat less expensive.

Enhanced quality of dialogue Assuming new willingness on both sides to move beyond the current model of NATO-Russia dialogue, the following measures can be suggested:

• Convene a high-level NRC meeting to provide direction

Summit and ministerial-level contacts are not excluded by the April 2014 NATO Foreign Ministers decision on suspending practical cooperation with Moscow.8 Many NATO Allies would currently see a ministerial level NRC as a totally unacceptable ‘reward’ to Moscow. But in other circumstances such a meeting could be reframed not as ‘business as usual’ but as ‘business that needs to be done’ to provide direction in reducing risk in a continuing adversarial relationship. It might be convened, for example, to address the ‘rules of the road’ for stability or even to give momentum to a stabilisation and deescalation process.

• **Establish a dialogue on cyber activities within the NRC**

There are no commonly accepted rules guiding NATO-Russia conduct in cyberspace and response towards hostile cyber activities. At the same time, there are several cyberrelated risks and challenges relevant to the NATO-Russia relationship: the risk of crossdomain escalation; the risk to command and control, communication, and early warning systems; the possibility of wrong or politicised attribution of a cyber-attack; the problem of third-party attacks and the lack of deterrence rules in cyber space. **A formal dialogue could serve transparency, confidence building and risk reduction.**

NATO and Russia could establish an NRC Cybersecurity Working Group to discuss possible risks involved in cyber activities and ways to mitigate their escalation. This certainly falls into the category of ‘**business that needs to be done’**. This group could start by working on a cyber-domain glossary of terms. Both parties could also work on a prohibition of cyber-attacks on command and control infrastructure. NATO and Russia could also use the working group to provide some transparency regarding their cyber policies and the mechanisms and criteria they will use to assess alleged cyber-attacks.

In the event of any future updates of the Tallinn Manual, which aims to identify rules for cyberspace activities, the facilitator – the NATO Cooperative Cyber Defence Centre of Excellence – could potentially invite Russian experts to participate, in order to broaden the range of the exercise.

#### Cyber hotline solves

Banco 19 Erin Banco National Security Reporter. Kevin Poulsen Sr. National Security Correspondent. Updated Mar. 07, 2019. “U.S. intelligence officials are looking to Washington-Moscow hotline as a last-ditch crisis channel that might just prevent a cataclysmic online showdown.” <https://www.thedailybeast.com/this-hotline-could-keep-the-us-and-russia-from-cyber-war> {DK}

As concerns mount that Russia will unleash hackers and online disinformation brigades to wreak havoc in another American election, senior U.S. officials are taking a second look at a technology handed down from the age of Gorbachev and Reagan: an emergency “hotline” between officials in the U.S. and Russia that might someday pull both countries back from the brink of an all out cyberwar.

The secure messaging system, known colloquially in the White House as the “cyberhotline,” already exists. It was set up in 2013—building off a Cold War messaging system, in fact—in the hope that it might facilitate conversations between the two countries during a crisis in cyberspace, where the identities and intentions of attackers are often muddled. So far it’s been used only once, in the waning days of the Obama administration, when the White House’s cyberchief fired off a carefully worded warning to Moscow not to attack the “infrastructure” for the 2016 election.

Since then, the U.S. has invested in developing a Cold War-style deterrence capability in cyberspace, and military brass have publicly touted their willingness to respond to foreign cyberaggression in kind. But with that sharper stick comes greater risk of a misunderstanding that might lead to an escalating conflict online. So intelligence officials in the Trump administration are talking about using the cyberhotline as a last-ditch crisis channel that might just prevent the electronic equivalent of the Cuban Missile Crisis, according to three U.S. officials.

“Everything has been laid out on the table, all sorts of options of dealing with this cybersecurity threat. The hotline is something that came up in the context of us needing to really face this issue head on—and to know that Russia has received the message,” said one senior intelligence official. “It’s the option we would use if we felt like all the other options weren’t working and if the crisis was escalating quickly. We’ve seen no signs that Russia has stopped meddling."

There are ongoing concerns in the Department of Homeland Security and the Federal Bureau of Investigation that Russia, among other countries, is continuing to stir trouble in U.S. politics and is actively planning to meddle in the 2020 presidential elections, according to three individuals with first-hand knowledge of reports drawn up within the last six months. (The FBI declined to comment for this story, and DHS didn’t respond to multiple written and telephone requests for comment.)

But while the Justice Department continues its prosecutions of Russian intelligence officers for their roles in the 2016 election and the military continues to prepare for a possible cyberwar, national security policymakers are grappling with a pair of beyond-thorny questions: How do we stave off another Russian attack on U.S. elections? And what do we do to keep any attack from becoming a cataclysm? Warning Russia directly through an official channel could provide at least some answers.

“I would expect to see some of that same Russian activity to occur again. I think the hotline is a useful tool to raise concerns,” said Michael Daniel, the former White House cybersecurity adviser and president and CEO of the Cyber Threat Alliance. “I am certain at some point the U.S. will use it again.”

Daniel was there for the first and only time the hotline has been used so far.

It was October 2016, not long before the voting for president was set to begin. According to Daniel, the Obama White House decided to warn President Vladimir Putin that it had gathered intelligence that indicated Russia was attempting to disrupt the U.S. election.

"We didn’t have full knowledge and understanding of the scope of the social media and disinformation work,” Daniel said. “We were focused on the threats to the actual infrastructure.”

The decision to contact Russia through the established hotline included a slew of top-level cabinet secretaries, including then-National Security Adviser Susan Rice.

Discussions about when and how to contact Russia spanned weeks, according to four former National Security Council staffers.

“There was a process at the staff level to approve the actual content to make sure we were sending the right message,” Daniel said, adding that no one in the administration knew if or how Russia would respond to the communication.

“The fact that we were using it to communicate our concerns about the potential for Russia using cyber-means to disrupt the election,” he added. “We knew it would convey how serious we were about this issue.”

The message, which was carefully crafted into an agreed template between the U.S. and Russia, eventually made its way to staffers at the Nuclear Risk Reduction Center (NRRC) at the State Department.

The U.S. and Russia created the center in 1987 as a way to establish a direct line of communication in the event of looming nuclear war. More than a quarter-century later, Washington and Moscow signed an agreement to establish the cyber hotline—one tacked on to the old NRRC messaging system and an additional voice line that would extend between the U.S. Cybersecurity Coordinator in the White House and the Russian Deputy Secretary of the Security Council.

“It was a big deal… just like in the cold war, the way you handle nuclear, and now cyber, is to ease involuntary escalation,” said Chris Painter who served as the top U.S. “cyber diplomat” at the State Department from 2011 to 2017.

Once the 2016 message left the NRRC system, Daniel and his team received notice that it had been delivered to the Kremlin.

“And then, we waited,” Daniel said, adding that everyone involved in the crafting of the message went back to their daily routines.

“It took a couple of days,” he said. “Then, we heard back. Their message was, ‘We need more information.’ That was the last of the communication.”

Two other former National Security Council staffers said that a voice hotline was also used to communicate with the Kremlin about election meddling.

The cyberhotline idea came to fruition in 2013 amid growing concerns in the U.S. administration that its relationship with Russia was on a crash course.

“The hotline was a symbolic gesture that could be used to help build a relationship with Russia and in the event of a real emergency, the administration and Moscow could… chat,” said one former State Department official.

The voice line, Painter said, “was something the Russians wanted… **No matter how bad things get** between Russia and the United States, **it is always answered**.”

## CP Solvency --- State Department

#### CP solves --- state department can share cyber intelligence with allies

Ford 22 --- Christopher A. Ford, Distinguished Policy Advisor at MITRE Labs and a Visiting Fellow at Stanford University’s Hoover Institution. He previously served as U.S. Assistant Secretary of State for International Security and Nonproliferation, “Conceptualizing Cyberspace Security Diplomacy”, SPRING 2022, <https://cyberdefensereview.army.mil/Portals/6/Documents/2022_spring/03_Ford_CDR_V7N2.pdf?ver=jPNxXAqiUZX7kFHLgxwpUw%3D%3D>

A less well known but growing component of the West’s cyber defense, however, is also diplomatic, in the form of cyberspace security diplomacy. As exemplified by the U.S. State Department’s Office of the Coordinator for Cyber Issues (CCI)5] this work involves engaging with foreign counterparts to develop and articulate common understandings of peacetime norms for cyber activity; this includes the principles set forth by United Nations experts in 2013 that states should not attack each other’s civilian critical infrastructure in peacetime.[6] It also involves promoting the adoption of common positions in attributing cyberattacks to malicious cyber actors and in imposing penalties (e.g., sanctions, public condemnation, or prosecution) upon those actors.

Cyberspace security diplomacy was responsible for a 2019 agreement reached by 28 Western countries expressing support for the “evolving framework of responsible state behavior in cyberspace,” supporting “targeted cybersecurity capacity building to ensure that all responsible states can implement this framework and better protect their networks from significant disruptive, destructive, or otherwise destabilizing cyber activity,” and pledging to “work together on a voluntary basis to hold states accountable when they act contrary to this framework.”[7] It is now not unusual for US officials to impose sanctions upon malicious cyber actors in other countries, nor for US law enforcement agencies to issue criminal indictments.[8] Work by US diplomats, intelligence officials, and law enforcement officers to engage their international counterparts, moreover, has helped encourage foreign governments impose concrete international steps to penalize such malefactors as well.[9]

In the US, such cyber-diplomacy has been undertaken under the aegis of the 2018 National Cyber Strategy, which called for “an international Cyber Deterrence Initiative” that would include building “a coalition [of states] and develop[ing] tailored strategies to ensure adversaries understand the consequences of their own malicious cyber behavior.”

The United States will work with like-minded states to coordinate and support each other’s responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.[10]

Such diplomacy cannot solve all today’s problems of rampant cybercrime and state-sponsored cyber assaults, of course, but it is a key piece of the puzzle as Western societies build effective responses.

Cyber diplomacy involves convincing others to agree upon cyber threat assessments, the attribution of specific attacks to specific actors, and what sorts of response may be appropriate in any given case. While there are extremely technical aspects of this work (such as the analysis of cyber-attackers’ TTPs and intelligence-derived information in connection with attribution assessments) cyber diplomacy is not only a technical matter but also a persuasive and even political exercise, in which international counterparts work to develop areas of agreement and decide upon courses of action. Because cyberspace security diplomacy is a relatively new field, though, little study has hitherto been done of the persuasive aspects of this work.

The Diplomacy of International Cyber-Collaboration

Cyberspace security diplomacy revolves heavily around international efforts to come to agreement on cyber threats – and on the attribution of a cyber-attack to a particular malicious cyber actor. “Attribution diplomacy” is critical to the State Department’s cyberspace security engagements. Though the conventional wisdom used to hold that such attribution was all but impossible in cyberspace,

… [i]t actually is possible to do more by way of attribution than most observers once thought possible. It is sometimes even possible to share enough information with one’s friends and partners that they, too, can have a reasonable degree of confidence in the source of an attack.[11]

## K Links --- Security

#### Use of the terms hybrid war and gray zone turn the case -- blurs the boundaries between war and peace and cause policymakers to think war is inevitable -- alt solves.

Stoker and Whiteside '20 [Donald and Craig; Winter 2020; Professor of Strategy and Policy for the US Naval War College's Monterey Program at the Naval Postgraduate School in Monterey; associate professor of National Security Affairs at the U.S. Naval War College at Naval Postgraduate School, senior associate with NWC’s Center on Irregular Warfare and Armed Groups, fellow at the International Centre for Counter-terrorism; "Gray-Zone Conflict and Hybrid War-Two Failures of American Strategic Thinking," Naval War College Review, Vol. 73, Issue 1, p. 19-54]

Among today's great ironies is that, despite the fact that the United States has been at war for the better part of two decades, rare is the American policy maker who speaks adeptly about our use of military power in a coherent manner. On the one hand, political leaders attempt to avoid categorizing our air strikes and raids targeting al-Qaeda and the Islamic State in countries around the world as war, while on the other hand they conflate hostile Russian acts with some form of hyphenated war. This article argues that the adoption of two prominent and fashionable theoretical terms and their various iterations-the gray zone or grayzone conflict (usually described as the space between peace and war) and hybrid war (often described as Russia's new form of mixed-methods warfare birthed by General Valery Gerasimov)-is an example of an American failure to think clearly about political, military, and strategic issues and their vitally important connections.

These terms, as well as the concepts arising from them, should be eliminated from the strategic lexicon. They cause more harm than good and contribute to an increasingly dangerous distortion of the concepts of war, peace, and geopolitical competition, with a resultant negative impact on the crafting of security strategy for the United States and its allies and partners around the world.

If an effort to eliminate two such commonly accepted terms and the theoretical approaches arising from them seems a fruitless effort to corral the contents of Pandora's box, then examine the most recent U.S. National Security Strategy and National Defense Strategy.1 You will not find either term in these documents even though, as we will see, both have appeared regularly in U.S. political and strategy documents for years. This demonstrates that it is possible to discuss security challenges without reliance on problematic terms that confuse strategic issues rather than clarify them. This is what we hope to achieve in this article.

There are four key problems with gray-zone conflict and hybrid war and the related variations of each.

1. They are examples of poorly constructed new theories that more often than not cloud rather than clarify.

2. They distort or ignore history, sometimes by claiming to be new when we have seen similar confusion in the past.

3. They feed a dangerous tendency to confuse war and peace.

4. They undermine U.S. strategic thinking via the construction of critical political and strategic documents on the basis of flawed ideas, even sometimes resulting in strategic guidance derived from a focus on tactical matters.

After almost two decades of war, we should heed the lessons that writers such as Emile Simpson learned firsthand in Afghanistan: "What liberal powers do by blurring the conceptual boundaries between war and peace is often to militarise in a polarised manner pre-established patterns of political activity, which might otherwise not be part of the wider conflict."2 As we will see, part of the cure for a poor understanding of some of our geopolitical problems is not to confuse geopolitics, competition among adversaries, or ham-handed influence efforts with war. The United States (and its allies) survived the Cold War (what some have termed more accurately the Cold Peace) without confusing whether it was at war or at peace with the Soviet Union-when such confusion could have produced nuclear Armageddon. We need to relearn how to make this distinction.

A FRAMEWORK FOR ANALYSIS

To support these claims, we must do something of fundamental importance: establish the basis for our discussion. This will give us a firm foundation for analysis, because without a secure base one cannot evaluate terms and concepts consistently and rationally. This is important because what some advocates of hybrid and gray-zone ideas are doing is elevating the importance of these concepts to being a new /theory of war. Proposing supposedly new tools or methods for analysis is to present new theory. How do we judge whether this theory is valid, rigorous, and testable?

Carl von Clausewitz gave us the first steps. "The primary purpose of any theory is to clarify concepts and ideas that have become, as it were, confused and entangled"3 Theory, as Sir Julian Corbett tells us, "can assist a capable man to acquire a broad outlook" Theory should teach us to think critically, to analyze, to bring a questioning but informed eye to the problem at hand, and to consider both its depth and breadth. It provides conceptual tools and grounds us by defining our terms and providing us a firm foundation for analysis, while teaching us to distinguish between what is important and what is not.4

The results of theory, Clausewitz insists, "must have been derived from military history, or at least checked against it" thus ensuring "that theory will have to remain realistic. It cannot allow itself to get lost in futile speculation, hairsplitting, and flights of fancy" Most importantly, particularly in any theory addressing warfare, it "is meant to educate the mind of the future commander"5 Historian Peter Paret has made similar points. "A theory that is logically and historically defensible, and that reflects present reality, has the pedagogic function of helping the student organize and develop his ideas on war, which he draws from experience, study, and from history-the exploration of the past extends the reality that any one individual can experience"6

#### Bad strategic studies terminology turns the case.

Stoker and Whiteside '20 [Donald and Craig; Winter 2020; Professor of Strategy and Policy for the US Naval War College's Monterey Program at the Naval Postgraduate School in Monterey; associate professor of National Security Affairs at the U.S. Naval War College at Naval Postgraduate School, senior associate with NWC’s Center on Irregular Warfare and Armed Groups, fellow at the International Centre for Counter-terrorism; "Gray-Zone Conflict and Hybrid War-Two Failures of American Strategic Thinking," Naval War College Review, Vol. 73, Issue 1, p. 19-54]

Commentators frequently use the gray zone phrase to describe the war Vladimir Putin launched against Ukraine in 2014, implying that the actions were opaque enough to cloud perceptions about whether war had erupted in the Donbas. Commentators also use gray zone and its variations to describe China's moves to cement its extralegal territorial claims in the South China Sea against weaker opponents, as well as Iranian moves in Syria and the Persian Gulf.

The popularization of the term gray zone appears to have been inspired by its incorporation into military documents and speeches. The 2010 Quadrennial Defense Review references challenges that occur in an "ambiguous gray area that is neither fully war nor fully peace."16 But it took the remarks delivered five years later by General Joseph L. Votel, USA, the then head of Special Operations Command, to bring the term into the public eye. He incorporated the concept into his briefing to Congress on the unique challenges posed by Russia and the Islamic State, noting that "our success in this environment will be determined by our ability to adequately navigate conflicts that fall outside of the traditional peace-or-war construct"17

An article discussing "a 'gray zone' between traditional notions of war and peace" appeared soon after.18 More publications quickly followed; they seem to be an elaboration of General Votel's remarks and to discuss conflicts "that fall between the traditional war and peace duality"19 Collectively, this work gave us a generally accepted definition of the term. Other publications arrived before the end of 2015.20 After these instances, use of the term exploded.21 One article arguing for a place between peace and war did appear in August 2014, but it does not mention a gray zone specifically.22 The earliest example of this delineation (which does not appear to underpin the key relevant literature) appeared in a 1995 international law article that mentions "the gray zone between war and peace"23 Japan's 2010 and 2013 National Defense Program Guidelines took a slightly different tack, pointing out that "there are a growing number of so-called 'gray-zone' disputes-confrontations over territory, sovereignty, and economic interests that do not escalate into wars"24 There is also a related October 2014 Stars and Stripes article.25

The key academic text seems to be Michael J. Mazarr's Mastering the Gray Zone, which does not provide a sufficiently clear definition of the gray zone. The best that can be derived from it is that a "new standard form of conflict" is emerging from "revisionist states" that are "competing below the threshold of major war."26 Moreover, gray-zone war is defined in relation to an undefinable term: major war.27 A commonly accepted definition of this in certain academic circles is as follows: "Major war means an operation where the United States deployed over fifty thousand troops and there were at least one thousand battle deaths."28 This definition is arbitrary and means based, and thus unusable.

Mazarr derived the term-at least in part-from the work of the special operations community.29 But our inquiries have failed to determine any inspiration for other recent American users of the term. It could derive from a 2005 book by Michael Hardt and Antonio Negri, American and Italian Marxist scholars, respectively (Negri is a devotee and former student of Michel Foucault). Hardt and Negri related the gray-zone concept to the post-Saddam Iraqi insurgency and wrote that "most of the current military engagements of the United States are unconventional conflicts or low-intensity conflicts that fall in the gray zone between peace and war"30 Ironically, here gray zone is used by critics of America to describe what is seen as deliberate efforts to blur recognition of what is clearly a military action: the occupation of a sovereign nation. Even more ironically, Russian officials frequently depict hybrid war as something "the Americans do" with "their advocacy of color revolutions"-which demonstrates the crossover contagion effects of the use of both terms.31

GRAY-ZONE CONFLICT AND THE CONSTRUCTION OF THEORY

There are several fundamental problems with use of the term gray zone.32 The first has to do with theoretical considerations. Again, the advocates of the concept-whether or not they realize it, and whether or not they insist they are doing so-are creating new theory about what is and is not war.33 The advocates of the gray-zone conflict terminology fail this test because, as we will see, they are not clarifying concepts but instead creating confusion.

As with some discussions of hybrid war, gray-zone publications haphazardly swirl and mingle the levels of war. Mazarr mixes strategy and tactics when he calls Chinese actions in the South China Sea the "use of gradual, multi-instrument strategies" then in the next sentence states that Russia's moves against Ukraine "also constitute a variety of the tactic" and in the next sentence avers that Iran's search for regional power and nuclear weapons is "a variety of gray zone strategy" He also writes that "gray zone conflict involves the holistic application of a mosaic of civilization and military tools, short of combat operations, to achieve gradual progress toward political objectives." Here, as in other places, the author is partly writing about grand strategy, because he is examining the various tools of power a nation can employ in pursuit of its political objective.34

All this produces a critical problem in logic. If you do not define your terms and stick to a valid use of them, you have not presented a basis for rational discussion. Failing to differentiate among grand strategy, strategy, operations, and tactics compounds this problem. A challenge on the tactical level must be addressed in ways starkly different from those applicable to a strategic threat.

Mazarr also argues that revisionist powers "are creating a new approach to the pursuit of aggressive aims, a new standard form of conflict" by undermining foes gradually on their periphery.35 The reality is that there is nothing new here. The Nazis used subversion to undermine Austria and Czechoslovakia before World War II. This was a standard Soviet practice against NATO countries. Mazarr himself writes that the ancient Greeks behaved in the manner now associated with gray-zone conflict. Revisionist or aggressive powers certainly are a problem today, but they always have been a problem and always will be.

None of this, of course, counters the fact that Mazarr and others indeed are correct about the danger from revisionist states. But we must parse the problem in a clearer manner to develop proper responses. If one identifies the problem incorrectly, one very likely will deliver the wrong answer. The most important and useful part of Mazarr's text provides superb analysis of the threat to the international order from several aggressive, revisionist powers. The challenges from China and Russia today resemble those of the 1950s. Both the Soviet empire and China had, on their respective borders, weak states that were not tied to any alliance system. Both also had revolutionary, and thus revisionist, regimes, as does Iran. Today, Russia, China, and Iran all have weak, often unaffiliated states on their borders, or ungoverned or disputed areas, such as parts of the South China Sea. The methods one uses to go about obtaining control of these areas fall under the realms of grand strategy, strategy, operations, and tactics. It is also here where the ideas of the original gray-zone writers, as we will see shortly, are very applicable.

The gray zone, as Adam Elkus observes, is "just another example of the strategic studies community needlessly confusing itself by generating new terminology to replace what is not broken"36