### **Democracy Answers**

#### **Democracy is resilient but fails**

Doorenspleet, University of Warwick Politics professor, ’19

[Renske Doorenspleet, Politics Professor at the University of Warwick, “Conclusion: Rethinking the Value of Democracy,” Rethinking the Value of Democracy, Springer Berlin Heidelberg, 2019, pp. p. 239-243]

Key Findings: Rethinking the Value of Democracy

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 database 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 frst fiding 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 fnding is that the instrumental value of democracy is very questionable. The feld 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 benefts 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 fourishing 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 diffcult, 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 specifcally, 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 confict 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 fghting 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 signifcant 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-ftsall 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 suffcient 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 benefts—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 favourable economic factors in a country—are much more powerful to explain the expected benefts, 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

#### **Resilience measures push people to give up their basic freedoms hurts democracy**

Atkinson, eSchool Security Studies Professor, ‘18

[Carol Atkinson, PhD, IR, Duke University, Professor, Security Studies, eSchool of Professional Military Education, and Lt. Col. (ret.), USAF, “Hybrid Warfare and Societal Resilience: Implications for Democratic Governance,” INFORMATION AND SECURITY: AN INTERNATIONAL JOURNAL v. 39 n. 1, 2018, p. 72-73]

U.S. citizens are not alone in acquiescing to increasingly intrusive government surveillance and monitoring. The governments of France, Germany, United Kingdom, Netherlands, Austria, Denmark, Finland, Norway,38 and Switzerland 39 have all recently deliberated or passed laws allowing greater surveillance of their own populations. A recent analysis by journalist Hugh Eakin concluded, “the very qualities that have made Sweden and Norway successful models of advanced democracy may also have made their populations more susceptible to government spying. In Norway, the government committee that put forward the mass surveillance legislation now before parliament has argued that such measures ‘can be justified as necessary in a democratic society’.” 40 This is an argument that seems to resonate and be accepted by citizens across Western democracies. This gradual relinquishing of democratic freedoms is a result of hybrid warfare strategies. It is a phenomenon that requires much more attention from scholars and democratic citizens alike.

Conclusion

Hybrid warfare presents a conundrum for Western democracies and their citizens. Increasingly, these governments have argued that their ability to counter cyber threats and “irregular” agents such as terrorists depends on the government’s ability to monitor all forms of communication, information and social connections on the internet and through cellular networks. This paper has suggested that the willingness of citizens to support government surveillance programs will ultimately undermine the basic freedoms that define what it means to be a democratic country. Hybrid warfare has opened a new era for international politics and Western democracies as democratic governance is undermined not only by hybrid warfare threats, but also by actions taken by democratic governments to counter those threats.

### **Democracy Answers**

#### **No democracy impact—too many other causes and does not prevent war**

Bennett, journal editor, ‘18

[Jonah Bennett, editor-in-chief, “The Rise and Fall of Liberal Democratic Peace Theory.” PALLADIUM MAGAZINE, 10—15—18,

<https://palladiummag.com/2018/10/15/the-rise-and-fall-of-liberal-democratic-peace-theory/>.

But something happened in the early 2000s. The unfolding of history as liberalism had been disrupted. The attacks of September 11, the subsequent bungling of intelligence regarding WMDs, the United States’ decision to drag its NATO allies into a series of embarrassing and ultimately ineffectual wars in the Middle East, numerous botched attempts at regime change and nation-building, and aggressive ideological demands as pre-conditions for diplomacy, have devastated the credibility of the U.S.-driven, Western liberal order. In some areas, history is now forking from the liberal path with a surprising confidence. Axios declared 2018 the year of the strongman, but it can also be called the year of liberalism in crisis. Russia, Egypt, China, Poland, Hungary, the Philippines, and Turkey—among others—have gained a renewed sense of self and conviction in their opposition to liberalism, as opposed to merely carving out for themselves an unprincipled exception to liberalism and ceding it the moral high ground. Even in Europe, where liberal democracy claims some of its greatest accomplishments, liberalism is beginning to unravel on the periphery in countries like Poland, Hungary, and Italy. Jair Bolsonaro, who notably expressed sympathy for a military dictatorship, has done tremendously well so far in the Brazilian presidential election. Neither soft, nor hard evangelism of liberalism is working the way it used to. For liberal theorists, the prospect of a liberal democratic world peace is now questionable. The Economist has put out a call to arms to defend liberalism as the most successful idea of the last 400 years. Whether this call results in anything substantial remains to be seen. But there is a palpable sense that liberalism is facing a serious new opposition. Despite this trend, liberalism’s theorists have a hope encapsulated by Daniel Deudney and G. John Ikenberry’s 2009 pronouncement that “liberal states should not assume that history has ended, but they can still be certain that it is on their side.” And yet, in the nine years following this bold pronouncement, history has not been especially kind to liberalism. Texas A&M political science professor Christopher Layne, writing in early 2018, has summed up the current situation aptly, namely that China as an increasingly self-aware superpower is already reshaping the world order away from Pax Americana: The US foreign policy establishment does not grasp this, and, instead, has invested the idea of a ‘rules-based, institutionalized’ international order with a talismanic quality. It claims that rules and institutions are politically neutral, and, ipso facto, beneficial for all. However, in international politics, who rules makes the rules. Rules and institutions reflect the distribution of power in the international system. A power transition is taking place in the early twenty-first century: US power is in relative decline and China is rising quickly. No international order—not even the Pax Americana—lasts forever. The liberal world order cannot survive the erosion of US hegemonic power. It is this structural change, not Donald Trump, that threatens the post-Second World War international order’s survival. It requires a huge leap of faith to believe that a risen China will continue to subordinate itself to the Pax Americana. Which brings us to the question: given that the prospect of an expanded democratic peace is starting to hit some hard limits, how well does liberal democratic peace theory actually explain the peace that has existed among liberal democratic states? Although LDP theory is taken as an empirical law in international relations, it has picked up a number of qualifications, making the theory far less interesting than first presented. Here are various renditions of the theory since its modern inception in the 1960s: Claim 1: liberal democracies go to war less than non-liberal democracies. The most significant abandonment in the field has been of the monadic hypothesis: that liberal democratic states are less likely to go to war compared to non-liberal democratic states. Henry Farber and Joanne Gowa have convincingly shown that, statistically, democracies on average have the same probability of going to war as non-democracies. At this point, no one holds the monadic hypothesis. Claim 2: no liberal democracy has fought another liberal democracy since 1816 (notably after 1812) This claim from Michael Doyle has increasingly fallen out of favor. There weren’t many democracies prior to 1945, and so the number of dyadic pairs of liberal democratic countries that could have gone to war was extremely limited. For example, Doyle excludes Great Britain from counting as a liberal democracy until 1832 and denies that the Spanish-American War of 1898 should count, even though the Polity II data set lists Spain as a democracy in 1898. Others have argued that the Second Philippines War of 1899 shouldn’t count either, as at the time the Philippines hadn’t held an election yet. This strong claim has largely been dropped because of a) exception cases that require new qualifications to explain, and b) the fact that there weren’t enough existing liberal democracies to achieve significance. All totaled, there are around 50 exception cases suggested in the literature. Claim 3: mature liberal democracies tend not to go to war/don’t go to war with one another Although Peru and Ecuador fought while both were liberal democracies, some maintain that the war occurred before the “pacifying effects” of liberal democracy had enough time to work, meaning maturity was lacking. Yet another qualification. Interestingly, the U.S. intervened militarily to topple Salvador Allende after he was democratically elected in Chile. Israel invaded Lebanon in 1981, but at the time, Lebanon’s government was in disarray. R.J. Rummel states that the Israeli attack on the United States’ USS Liberty in 1967 counts as conflict below the level of war, but argued that Israel at the time was “only partially free.” That Finland joined up with the fascists from 1941 to 1944 apparently shouldn’t count, as no Finnish troops attacked troops from a liberal democratic country, though Great Britain bombed Finland in 1941. Claim 4: mature liberal democracies in the post-1945 era don’t go to war with one another The addition of the ‘post-1945 era’ qualification came later in the development of LDP theory, and while it may be a disappointing qualification, it may be necessary, given the small-N universe of liberal democracies before 1945. Bruce Russett admits that “the absence of murderous quarrels between democracies was not too surprising, and may need—at least for the pre-1945 era—little further explanation.” Claim 5: mature liberal democracies in the post-1945 era don’t go to war with one another, but for normative reasons, not structural reasons It’s claimed that the structural elements of liberal democratic states, namely separation of powers, checks and balances, elections, the free press, etc. should result in less war in general, but this is essentially equivalent to the monadic hypothesis, which has been largely abandoned. So, it might be possible to explain the absence of war through the normative mechanisms of liberal democratic states, as opposed to structural elements. Zeev Maoz and Bruce Russett argue that while there is some support for the structural model, the normative model has more support and better consistency. The above examples illustrate continuing iterations of the theory. This trajectory is by no means perfectly linear, nor is there consensus on how many qualifications are required, but the fact that these qualifications have continued to pile on is evidence that LDP theory is now much closer to triviality than when first introduced.

#### **The aff can’t solve the demise of democracy – Sustained educational, national, and community investments are key**

**Miller-Idriss, 21** -- Miller-Idriss, C. (2021, November 25). *America's democracy is failing - and the World Knows it*. MSNBC. Retrieved June 20, 2022, from https://www.msnbc.com/opinion/america-s-democracy-failing-world-knows-it-n1284597

Luckily, just because a democracy is in crisis does not mean it will collapse. On average, **it takes** [**about a decade**](https://web.archive.org/web/20210328045720/https%3A/www.idea.int/sites/default/files/publications/chapters/conditions-and-consequences-of-populism-and-democratic-backsliding.pdf)from the onset of democratic backsliding to end in either democratic breakdown or recovery. But we are long overdue for a course correction. Aside from international NGOs focusing on fixing America’s democracy, we can learn from the experiences of foreign governments throughout history, too. Germany’s post-World War II efforts to strengthen democracy include a wide variety of investments that simultaneously tackle right-wing extremism, racism, and antisemitism. South Africa built a national Truth and Reconciliation Commission to address the atrocities of apartheid and provide a path to restorative justice and healing. These cases demonstrate that it is possible — with sustained educational, national, and community investments — to create more informed citizens, restore trust across dividing lines, energize youth engagement, and reduce political violence. Doing so requires significant educational and [media literacy](https://www.npr.org/2019/03/22/705809811/students-in-ukraine-learn-how-to-spot-fake-stories-propaganda-and-hate-speech) programming. It requires engagement across sectors, through partnerships with civil society, the tech and media sector, local governments, and faith communities. Ultimately, restoring democracy requires creating a nation in which every citizen and resident feels part of a shared community in which they have a voice and a path to a common future. We are a long way from that kind of shared community. And in the end, saving our own democracy will require more than the efforts of a few committed citizens. The kind of effort we need to turn our backsliding democracy around cannot be done if the federal government doesn’t lead the charge with serious resource investments. At its heart, this work is about resilience, rooted in an understanding that democracies must be nurtured through education and not just defended with force. After the terrorist attacks of 9/11, the U.S. made unprecedented investments in our security infrastructure. We created an entire new agency — the U.S. Department of Homeland Security — whose mission is to “[secure the nation from the many threats we face](https://www.dhs.gov/about-dhs).” But now, the call is coming from inside the house: the biggest threats to our nation are ones we’ve created ourselves.

**Imperialism Turn**

#### **The U.S. is using cyber security to expand their foreign oversight**

International Journal on Human Rights, July 2018, <https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/>

A simplistic analysis of the current situation of tensions between privacy and security (the prevalent narrative in media) will probably state the following: States are spying on national and foreign citizens and the trend will only increase as they acquire cheaper technologies, proportional to their military and technological power. The private sector does it too, but not with inherently bad intentions or political purposes. What the private sector is concerned about is the “experience” of the user and the maximum capture of their data and how to offer the best products and services. Collateral damage, such as the abuse of Facebook data, by companies like Cambridge Analytica, is the exception to the rule.2 As for the people, they are not really concerned about their government spying on them. They are somewhat concerned about private sector surveillance, but they are willing to allow it, especially if that enables them to enjoy “free” services or improve their overall experience. This is despite the fact that privacy awareness is gradually increasing and rules are slightly improving in some regions, especially in Europe for example after the entering into force of the General Data Protection Directive (GDPR), patching a broken system of systemic privacy erosion and data extractivism.

#### **The United States is imperialist already in cyber space, the AFF would make it worse**

Henning Lahmann, January 8, 2022, Lahmann is a Hauser Global Postdoctoral Fellow, NYU School of Law; Program Leader International Cyber Law, Digital Society Institute, ESMT Berlin; Associate Research Fellow, Geneva Academy of International Humanitarian Law and Human Rights.https://deliverypdf.ssrn.com/delivery.php?ID=859095117066065115097126117125098112023069025084090022029083126123074075073025065085045043007017025043026064097121071070019002046002027035000099000115004091122115097068050008064105006004087000102000127096087090123108073116015086066108112083011082125120&EXT=pdf&INDEX=TRUE

After tracing the doctrinal origins of the interpretation of “respect for sovereignty” as a primary rule of international law, the subsequent sections examine three broad trajectories among states’ attitudes toward the status of sovereignty in cyberspace under international law. Before addressing the legal opinions of the growing number of states that have endorsed the “sovereignty-as-rule” position, I investigate two categories of states that, for political-ideological reasons, conceive cyberspace in ways fundamentally irreconcilable with this emerging consensus: “cyber imperialism,” embodied by the U.S. and its closest allies, and “cyber-Westphalia,” as represented by China, Russia, and Iran.

**Imperialism Turn**

#### **NATO is responsible for millions of innocent deaths around the globe.**

Lendman, 2020 (Stephen, a 2008 Project Censored winner and 2011 Mexican Journalists Club international journalism award recipient, June 9.) NATO’s Diabolical 2030 Agenda. <https://stephenlendman.org/2020/06/09/natos-diabolical-2030-agenda/>

NATO’s existence hasn’t “kept us safe for 70 years.” Its existence is responsible for countless millions of deaths, vast destruction, and human misery wherever its forces show up.

As long as the alliance exists, world peace and stability will remain unattainable.

The risk of global war with nuclear weapons will haunt humanity.

Washington wants NATO used as a global military to force its will on other nations belligerently, to crush democratic freedoms where they exist, to bludgeon or bully countries worldwide to bend to its will.

NATO 2030 is a scheme for expanding NATO worldwide more than already, for greater military spending, for crushing opposition to Washington’s imperial aims.

It’s an agenda that risks global war with nukes, Stoltenberg serving as a mouthpiece for diabolical US aims.

Taking orders from a higher authority in Washington, he’s charged with saluting and obeying.

Claiming China is a threat to US hegemonic aims, he said the following:

Its ruling authorities “are investing heavily in modern military capabilities, including missiles that can reach all NATO countries.”

NATO is all about militarization and warmaking, unrelating to “protecting each other” — despite no foreign threats to any alliance member states.

Disbanding NATO would be one of the most important ways to advance world peace and stability over endless wars US-led member states wage.

The alliance has always been all about offense, not defense, notably since the Soviet Union dissolved nearly 30 years ago.

US-controlled NATO is a killing machine, an aggressor alliance, an enemy of world peace and stability.

The kind of world it pursues is unsafe and unfit to live in.

As long as the alliance exists, so will a permanent state of war on humanity along with it.

#### **NATO is a tool for the Western war waging, its imperialist expansion agenda is a threat to humanity.**

Lendman, 2020 (Stephen, a 2008 Project Censored winner and 2011 Mexican Journalists Club international journalism award recipient, June 9.) NATO’s Diabolical 2030 Agenda. <https://stephenlendman.org/2020/06/09/natos-diabolical-2030-agenda/>

From inception, US-dominated NATO has always been and continues to be an instrument for advancing its imperial agenda by brute force — endless wars its favored strategy along with other hostile actions.

Alliance secretaries general operate as US puppets, serving its imperial interests, Jens Stoltenberg the latest in a long line of subservient NATO heads.

On Monday, he addressed the Washington-based Atlantic Council (AC), a neocon infested think tank involved in weaponizing hysteria against nations on the US target list for regime change — notably China, Russia and Iran.

AC’s board of director and so-called “experts” include a rogue’s gallery of hawkish extremists who never met a sovereign independent country they didn’t want transformed into a US vassal state by brute force or other hostile means.

NATO’s longterm vision is all about pursuing Washington’s imperial agenda globally. Stoltenberg’s mandate is furthering its diabolical aims.

Its 2030 agenda includes expanding the alliance worldwide, greater military spending, and more preemptive wars on humanity than already — a scourge essential to challenge.

At a time when the only threats face by the US and other Western countries are invented, not real, Stoltenberg pretends otherwise in deference to his master in Washington.

He lied saying “Russia continues its military activities unabated.”

Russian forces are in Syria by invitation of its legitimate government — involved in aiding its military combat US-supported ISIS and likeminded jihadists.

Stoltenberg: “ISIL and other terrorist groups are emboldened” — instead of explaining they’re US proxies in Syria, Iraq, Afghanistan, Yemen, Libya and elsewhere, used by the Pentagon and CIA.

### **Liberal Order Ans: Norms Fail**

#### **Can’t establish cyber norms**

Maurer ’19 [Tim Maurer, Co-Director, Cyber Policy Initiative, Carnegie Endowment for International Peace, “A Dose of Realism: The Contestation and Politics of Cyber Norms,” HAGUE JOURNAL ON THE RULE OF LAW, 2019, SpringerLink]

3.5 Part 5: Metacontestation Over the UNGGE Process

While some UN member states have criticized the UNGGE process as lacking legitimacy because of its limited membership, there are other forces tearing at the fabric of the regime that has been built around the UNGGEs. These criticisms can be considered a standalone metacontestation over the existing UN process writ large. Its critics question whether the UN process has been sufciently impactful, whether it is worth pursuing further, and whether it ought to be replaced with a diferent process. These arguments focus on (1) the broad scope and vague nature of agreements, (2) the inadequacy of addressing the deteriorating security environment, (3) the hidden agendas, including hypocrisy, of some stakeholders, and (4) the disconnect between those negotiating and those carrying out ofensive operations.

1. Broad scope and vague nature of agreements A common critique from ofcials in national security agencies is that the framework developed by the UNGGE is too broad and too vague to be truly effective at establishing rules of the road adhered to by those carrying out offensive cyber operations (Burgess 2018; Baker 2017; Fischerkeller and Harknett 2018). Their skepticism refects the still nascent and continuously maturing understanding of the technology’s impact on the balance of power, its use as an instrument of statecraft, and the security dilemma that is as present online as it is ofine. As an alternative approach, this group of stakeholders proposes to focus on agreements based on emerging state practice and more narrowly defined areas of common interest as the basis for cyber norms that could then be expanded over time (Fischerkeller and Harknett 2018; Fischerkeller 2018).

2. Inadequacy of addressing deteriorating security environment A separate point of critique of the UNGGE process makes the opposite argument. Instead of viewing the UNGGE’s framework as too broad and ambitious, this separate camp of critics argues that the UNGGE process has not been ambitious enough. They see a functional need for international cooperation among governments and transnational cooperation among nongovernmental actors to address the deteriorating cybersecurity environment. A leading voice of this group is the multinational company Microsoft. After years of being involved in international cyber norms discussions, Microsoft CEO Brad Smith elevated the company’s engagement to an unprecedented level by calling for a Digital Geneva Convention (Smith 2017; Meredith 2018). In the wake of the economic costs caused by the 2017 WannaCry and NotPetya, these voices have become louder with a growing number of CEOs joining the chorus (Greenberg 2018; Cybersecurity Tech Accord 2018; Siemens 2018). In addition, the UN Secretary General made the topic a priority in 2018 supporting a more ambitious agenda (Khalip 2018; Fidler 2018).

 This group of norm entrepreneurs remains very active trying to further advance the cyber norms discussion by keeping the pressure on governments.26 For example, Microsoft broadened its eforts beyond its engagement as a single company by creating the ‘Tech Accord’ consortium counting more than 70 global companies at the beginning of 2019 (Cybersecurity Tech Accord 2018). In late 2017, Siemens established a nonrival network of a dozen companies creating a ‘Charter of Trust’ focusing specifcally on supply chain integrity (Siemens 2018). Meanwhile, the Dutch government led the charge to add a norm protecting the core of the Internet to the list of norms agreed to through the 2015 UNGGE (Broeders 2016). The French government’s desire to maximize the impact of the Paris Peace Forum launched in 2018 at the 100th anniversary of the end of World War I led to the adoption of the Paris Call for Trust and Security in Cyberspace in November 2018 that explicitly references the norm to protect the core of the Internet (France Diplomatie 2018). The Paris Call has also been described as an umbrella framework for the activities of various norm entrepreneurs.27

3. Hidden agendas Those promoting a more ambitious agenda have encountered a number of challenges due to the dynamics among and within governments. First, among governments, calls for a treaty have been met with resistance by Western governments. Concerned about Moscow’s true intentions, these governments worry that any push for a treaty will empower Moscow’s longstanding proposal. Their concerns explain continued resistance by Washington and Western capitals with respect to the draft International Code of Conduct that Moscow and Beijing developed in 2011, updated in 2015, and have been promoting since (see McKune 2015.) They also help explain why Microsoft’s call for a Digital Geneva Convention has met similar resistance and illustrate that overcoming this path dependence would require exceptional circumstances. Second, within governments, national security agencies are reluctant to internalize and adhere to the norms refected in the UNGGE agreements due to the still nascent understanding of the domain, a related desire to preserve options until a mature strategic framework has emerged, and the dynamics of the security dilemma (Burgess 2018, Efrony and Shany 2018). A good illustration of this still maturing understanding of the technology is the argument promoted by some that there is moral obligation to use hacking instead of conventional weaponry if the efects of the former are less harmful than the latter (Hollis 2014).

4. Disconnect between those negotiating and those conducting ofensive cyber operations A fnal obstacle worth mentioning—rather in form of a hypothesis than conclusive analysis—is that a particular challenge for negotiating cyber norms may be that the conduct of ofensive cyber operations originated in and continues to be closely tied to intelligence agencies, the most secretive parts of any government (Smeets 2018). Until recently, their public engagement was minimal. For example, the acronym of the U.S. National Security Agency (NSA) has been commonly referred to as ‘No Such Agency.’ The bureaucratic culture of these agencies is therefore not infused with a history of interactions with their respective counterparts internationally (apart from the norms governing spy swaps that emerged during the Cold War.) Unlike the militaries of the world that—despite fghting each other—have developed norms for the exchange of prisoners, the treatment of the wounded, and other activity, this sort of interaction is not part of intelligence agencies’ DNA.28 With that said, the pace of change afecting intelligence agencies in the past 5 years alone is breathtaking with potential changing attitudes toward such interactions. For example, from the NSA to the Australian signals directorate, agencies now even have active Twitter accounts and terms such as Five Eyes have become household names (Australian Signals Directorate 2018).

#### **Liberal International Order norms are hollow and coercive – they’re a guise for endless intervention**

Staniland 18 --- PhD from MIT (Paul Staniland is Associate Professor of Political Science and Chair of the Committee on International Relations at the University of Chicago, “Misreading the “Liberal Order”: Why We Need New Thinking in American Foreign Policy,” July 29, https://www.lawfareblog.com/misreading-liberal-order-why-we-need-new-thinking-american-foreign-policy)//CMR

Pushing back against Trump’s foreign policy is an important goal. But moving forward requires a more serious analysis than claiming that the “liberal international order” was the centerpiece of past U.S. foreign-policy successes, and thus should be again. Both claims are flawed. We need to understand the limits of the liberal international order, where it previously failed to deliver benefits, and why it offers little guidance for many contemporary questions. First, advocates of the order tend to skim past the policies pursued under the liberal order that have not worked. These mistakes need to be directly confronted to do better in the future. Proponents of the order, however, often present a narrow and highly selective reading of history that ignores much of the coercion, violence, and instability that accompanied post-war history. Problematic outcomes are treated as either aberrant exceptions or as not truly characterizing the order. One recent defense of the liberal order by prominent liberal institutionalists Daniel Deudney and G. John Ikenberry, for instance, does not mention Iraq, Afghanistan, Vietnam, or Libya. Professors Stephen Chaudoin, Helen Milner, and Dustin Tingley herald the order’s “support for freedom, democracy, human rights, a free press.” Kori Schake writes that Western democracies’ wars are “about enlarging the perimeter of security and prosperity, expanding and consolidating the liberal order.” Historian Hal Brands argues that the order has advocated “political liberalism in the form of representative government and human rights; and other liberal concepts, such as nonaggression, self-determination, and the peaceful settlement of disputes.” Other analysts have persuasively argued that these accounts create an “imagined” picture of post-World War II history. Patrick Porter outlines in detail how coercive, violent, and hypocritical U.S. foreign policy has often been. To the extent an international liberal order ever actually existed beyond a small cluster of countries, writes Nick Danforth, it was recent and short-lived. Thomas Meaney and Stephen Wertheim further argue that “critics exaggerate Mr. Trump’s abnormality,” situating him within a long history of the pursuit of American self-interest. Graham Allison—no bomb-throwing radical—has recently written that the order was a “myth” and that credit for the lack of great power war should instead go to nuclear deterrence. Coercion and disregard for both allies and political liberalism have been entirely compatible with the “liberal” order. The last two decades have been a bumpy ride for U.S. foreign policy. Since 9/11, we have seen the disintegration of Syria, Yemen, and Libya, a war without end in Afghanistan, the collapse of the Arab Spring, the rise and resurgence of the Islamic State, and the distinctly mixed success of strategies aimed at managing China’s rise. At home, the growth of a national-security state has placed remarkable power in the hands of Donald Trump. Simply returning to the old order is no guarantee of good results. Grappling openly with failure and self-inflicted wounds—while also acknowledging clear benefits of the order—is essential for moving beyond self-congratulatory platitudes. Second, the liberal order in its idealized form had very limited reach into what are now pivotal areas of U.S. security policy: Asia, the Middle East, and the “developing world” more broadly. The core of the liberal order remains transatlantic, but Asia is now growing dramatically in wealth and military power. What is the record of the order in the region? There was certainly some democracy promotion when authoritarian regimes began to totter, but there was also deep, sustained cooperation with dictators like Suharto and Ferdinand Marcos; while there are some regional institutions (such as ASEAN), they are comparatively weak; while there are some rules, they have been deeply contested. Close U.S. allies like Japan, Taiwan, and South Korea (the latter two experiencing long bouts of U.S.-allied autocracy) were not integrated into a broad alliance pact like NATO. India and Pakistan were never part of the core order, and China was only very partially integrated (primarily into the economic pillar of the order, and through ad hoc security cooperation from the 1970s). Southeast Asia has been a site of warfare and authoritarianism for much of its post-1945 history. The United States has long considered the Middle East vital to its security, but the extent to which the United States should invest its own blood and treasure in protecting the area was always up for debate. It was only in the 1970s that the United States decided it was prepared to use force to defend the region; “dual containment” in the 1990s was always controversial, while the invasion of Iraq and its chaotic aftermath revealed deep fissures over how much presence was enough. Meanwhile, liberalism, democracy, human rights, and international institutions have not made much of a mark in the region. Jake Sullivan, in a rather odd defense of the order, suggests that “Middle Eastern instability has been a feature, not a bug, of the system.” This is not reassuring about the order’s ability to structure politics in the area. The same can be said about the order’s history in Africa, with deep Western involvement in civil wars, support for authoritarian regimes, and often-counterproductive demands for economic liberalization contributing to ongoing instability. The legacy of the “liberal order” is both far more complex and shallower outside of the north Atlantic core than within it. Invocations of the order are seen with greater cynicism and suspicion in these areas than in Washington or Berlin. Yet they are precisely the regions that are increasingly the focus of U.S. security policy. Finally, and as the preceding already suggests, the idea of “liberal order” isitself frequently too vague a concept, and was too incomplete a phenomenon, to offer guidance on a number of key contemporary questions. Allison goes so far as to call it “conceptual Jell-o.” The extremely abstract principles that experts use to define the order are confronted with a reality of extreme historical variation. This amorphousness undermines its usefulness as an actual guide to future foreign policy. U.S. alliances in Western Europe since World War II looked dramatically different than those in East Asia. Both have achieved their basic goals, so which should be the model for the future? The United States often applied pressure to coerce its allies into adopting economic and security policies conducive to U.S. interests—going so far as to threaten abandonment of close European allies—even as it simultaneously built key elements of the liberal order. The core of the liberal order was a more tenuous and contested political space than we often remember. This inconsistency applies to involvement in the domestic politics of other states. The United States has regularly embraced authoritarian leaders (and distanced itself from democratic regimes), while at other times it has helped to push these leaders out in the face of domestic mobilization. Advocates of the order tend to stress the latter and dismiss the former as aberrant, but both strategies contributed to the ultimate victory of the liberal order over the Soviet bloc. The order’s history offers support for aggressively promoting democracy, accepting democratization when it emerges, and strongly supporting friendly dictators. This makes it unhelpful for grappling with the question of whether and how to promote democracy. The same is true of military interventions and covert operations abroad. U.S. leaders invested heavily in Cold War proxy wars and the overthrow of foreign regimes, while at other times and places they avoided such interventions. This history carries important implications for addressing today’s policy challenges. Simply appealing to the order does not, for instance, tell us much about how to deal with a rising China: Since the liberal order included highly institutionalized alliances, loose “hub-and-spoke” arrangements, and coalitions of the willing, and was characterized by both preventive wars and containment, it is extremely unclear what the order suggests for America’s China strategy. While “rules-based” order is a term in vogue, it doesn’t tell us what the rules should actually be, or how they should be decided. Nor does appealing to the liberal order help us understand whether the United States needs to be deeply involved or largely absent from the Middle East, or somewhere in between. Under the order, democracy promotion and assertive liberal intervention sometimes occurred, but so too did restraint and an acceptance of autocracy. There are no answers in the liberal international order for navigating the enormously difficult terrain of the contemporary Middle East.

**Misinformation Answers**

#### **The alternative is no news**

Hurwitz ’17 [Justin Hurwitz, Assistnat Professor, Law, University of Nebraska, “Fake News Not-So-Real Antitrust Problem: Content Remains King,” Compeittion Policy International, 2017, <https://laweconcenter.org/wp-content/uploads/2018/01/CPI-Hurwitz.pdf>, accessed 10-5-21]

Nor are there vertical – or to use the antitrust newspeak, platform – concerns driving the problem of fake news. Facebook is a platform-based distributor of information, including news. This means that news is (one of many) inputs into Facebook. Hubbard suggests that Facebook’s gatekeeper position allows it to harm the traditional media in an effort to keep people on Facebook’s own site. She points, in particular, to Facebook’s use of its proprietary in-app browser and Instant Articles feature, arguing that Facebook uses these to lock users in to Facebook’s platform, denying third-party news sites valuable analytics and advertising revenue, and making it more difficult for users to navigate away from Facebook. As an initial matter, in-app browsers have become common. Facebook, Twitter, and Google News all use them. This suggests that they have been implemented to address a technological problem – to make the mobile browsing experience better for users of each platform. And, indeed, this is the case. Websites that have not been redesigned specifically for mobile platforms often do not work well.

Even websites that do have mobile versions often do not work particularly well. The user experience between those websites is often nonstandard, which inconveniences users and may encourage them to discontinue their use of both that website and the platform that sent them there. By using an in-app browser – and especially by offering a standardized format for presenting news content across sites in that browser – platforms can (at least in principle – I will not defend the quality of many in-app browsers, with the recognition that they are a new and improving technology) offer users a superior experience. This means that they will make more use of a platform, yes, benefitting, for instance, Facebook – but it also means that they will consume more content via that platform, benefitting, for instance, media outlets. Importantly, mobile browsing, where we see these in-app browsers, is different from browsing in a desktop environment. When a user is sent to a website for an article on a mobile device, they are unlikely to stay on that website once they are done with the article. Rather, they are likely to exit out of the browser, which sends them back to whatever source sent them to the website initially. This means that users are “locked in” to the Facebook platform no matter whether it uses an in-app or external browser. Hubbard is exactly right that in-app browsers and Instant Articles are an effort to keep users engaged with the Facebook platform. But the alternative is not users engaging more with news outlets’ platforms. The alternative is users getting frustrated with news outlets’ mobile experiences and finding more enjoyable ways to spend their time than waiting for poorly-rendered webpages to load. Facebook knows that if they can make articles quick and easy to access, more people will spend more time on their phones. This is why Facebook is willing to offer content providers a significant share of ad revenue. And, to the extent that publishers of any sort continue to produce content that Facebook users want to engage with, those publishers will continue to be able to demand such a share of revenue. Facebook has no incentive to deny its users access to content linked to via Facebook. To the contrary, it has every incentive to get them seamless access to that content, and is willing to pay to do so.

#### **Social media misinformation comes from all platforms, independent of cyber attacks**

**Burns, 2/9 --** Burns, G. (2022, February 9). *Journalists give thumbs down to social media*. Local News Initiative. Retrieved June 19, 2022, from https://localnewsinitiative.northwestern.edu/posts/2022/02/09/medill-social-media-survey/

Journalists say social-media platforms have hurt their industry, contributing to inaccurate and one-sided news accounts by exerting too much control over the mix of news that people see, according to a recent survey. More than nine of every 10 survey respondents said social-media companies deliver a “worse mix of news” to their users, according to the online survey of journalists by Northwestern University’s Medill school of Journalism, Media, Integrated Marketing Communications. The survey also found that nearly eight of 10 said harassment of journalists on social media is a “very big” or “moderately big” problem. The second-ever Medill Media Industry Survey was conducted at the end of 2021 by Associate Professor Stephanie Edgerly of Medill, and Danielle K. Brown, the Cowles Professor of Journalism, Diversity and Equality at the University of Minnesota. More than 1,500 members of the U.S. news media completed the questionnaire. Medill used Cision, a media listings database, to obtain email contact information from individuals who had at least one of the following keywords in their profile: columnist, correspondent, director, editor, producer, reporter, writer, then sorted the list for news organizations exceeding a minimal audience size. Exactly 25,000 people were invited to participate in the survey, which was open between Nov. 30 and Dec. 31. Among the findings, 90.7 percent of respondents said the role social media companies play in delivering the news results is a worse mix of news, while 86.5 percent said social media companies have too much control over the mix of news people see. Some 79.3 percent said social media has a mostly negative impact on the journalism industry, and an overwhelming 94.3 percent of respondents blamed social media for spreading **inaccurate news**. The survey was the subject of a discussion at a Medill Centennial panel on Feb. 3, featuring newsroom leaders of ABC News, The Wall Street Journal, Vox Media and the Los Angeles Times. “There’s certainly a lot of frustration,” observed Kevin Merida, Executive Editor at the Times. But Merida also said social-media platforms are an important gateway to the work of journalists, who must learn to operate on them. “We’re not putting the genie back in the bottle,” he said. “Within the platforms, we have the ability to also hop in and define our relationship, how we’re going to access them and how we’re going to communicate through them.” ABC News President Kimberly Godwin said journalists need to help people become smarter consumers of news on social platforms. “They keep sending you misinformation,” she said. “We have to find ways to break through the clutter so that they get at the truth.”

**Misinformation Answers**

#### **Journalists and news reporters already fighting to improve accuracy, reliability, and quality of news information on social media platforms**

**Burns, 2/9 --** Burns, G. (2022, February 9). *Journalists give thumbs down to social media*. Local News Initiative. Retrieved June 19, 2022, from https://localnewsinitiative.northwestern.edu/posts/2022/02/09/medill-social-media-survey/

Social media challenges journalists to understand its strengths and weaknesses so they can interest an audience and deliver strong, accurate messages, said Melissa Bell, publisher of Vox Media. “It is important for us to recognize how much of an impact social media has had on our reporting,” she said. “There are strengths in it. There are ways to reach people that you couldn’t reach before.” Journal Editor in Chief Matt Murray warned that journalists should not mistake dialogue on social media for the “richer, fuller, more varied and dramatic” stories that reporters can uncover in “real life.” “Social media is a tool, from a journalist’s perspective, to be used,” he said. “It’s a tool to get news out there,” Murray said. The survey indicates that journalists are more critical of social media than are U.S. adults at large. The percentage of U.S. adults saying the companies have too much control over the mix of news they see was 62 percent in a Pew Research Center survey from July 2019. That response was nearly 25 percentage points lower than that of journalists in the 2021 Medill survey. Similarly, the percentage of U.S. adults who said social-media companies provide a worse mix of news was 55 percent in the Pew survey, far less than the 90.7-percent response from journalists surveyed by Medill. Edgerly, who oversaw the survey, said its results suggest that social media is not living up to its potential to make vital news stories more visible. “A clear majority of journalists are seeing the potential gains are not matching the realities,” she said. “The survey suggests that we’re not seeing quality information reaching a broader audience. That is not the reality of how social media functions.” The University of Minnesota’s Brown, who partnered with Edgerly, said she’s not surprised that journalists’ view of social media is more negative than the population’s at large, as measured in other surveys. “We asked journalists to think about: social-media companies and their control; loss of autonomy; and how the work they create is used by other people,” she said. “It doesn’t surprise me that they don’t like the way social-media companies control the news that people have access to. It doesn’t surprise me at all.”

#### **Algorithms which run social media newsfeed preferences are biased towards outrage and views, thus promoting news regardless of its accuracy or reliability**

**Stewart, 20 --** Stewart, E. (2020, December 22). *America's growing fake news problem, in one chart*. Vox. Retrieved June 17, 2022, from https://www.vox.com/policy-and-politics/2020/12/22/22195488/fake-news-social-media-2020

There’s now [a running debate](https://www.theverge.com/interface/2020/7/22/21332774/facebook-crowdtangle-kevin-roose-nyt-tweets-interactions-reach-engagement) among academics, analytics experts, and observers like Roose around what we know about what’s happening on Facebook and why. Dartmouth political scientist Brendan Nyhan recently [argued](https://twitter.com/BrendanNyhan/status/1299166780913602560) that “likes,” comments, and shares are just a small part of what people actually see on Facebook, and that it’s difficult to draw conclusions from these interactions alone or to know what they might mean for an election. Still, the trend is concerning. [Social media is making political polarization worse in America](https://www.vox.com/recode/21534345/polarization-election-social-media-filter-bubble), and it’s often the case that people no longer agree on even basic facts. What people consume shapes what they see — basically, someone clicks on a certain article and algorithms start to predict what else they might like in alignment with that. And the further down the rabbit hole they go, the more they begin to seek out that media, often winding up in an information bubble. For people who complain so much about supposed social media censorship, they are not really being censored Republicans have spent years complaining that social media companies are biased against them and that their content is being censored and removed. President Donald Trump [has often lashed out](https://www.vox.com/recode/2020/5/28/21273878/trump-executive-order-twitter-social-media-section-230-free-speech-implications) against tech companies with unfounded claims of bias. He and his administration [have also attempted to undercut and scrap Section 230](https://www.vox.com/recode/2020/6/18/21294331/section-230-bill-barr-josh-hawley-trump-internet-free-speech), a law that basically says social media companies are allowed to police their platforms however they want and aren’t liable for the content third parties post on them. ([Recode’s Sara Morrison has a full explainer on Section 230](https://www.vox.com/recode/2020/5/28/21273241/section-230-explained-trump-social-media-twitter-facebook). Rather than bias toward a certain political leaning, social media algorithms are often biased toward outrage — they push content that people have an emotional reaction to and are likely to engage with. The NewsGuard data and other research shows that **people are increasingly being drawn to unreliable content** — and often, unreliable content that has a conservative bent. And that content can influence all sorts of attitudes and cause confusion on even basic facts. [The New York Times](https://www.nytimes.com/2020/12/22/technology/georgia-senate-runoff-misinformation.html) recently took a look at Georgia and how misinformation and unreliable news is playing a role in the [US Senate runoffs](https://www.vox.com/21571755/georgia-senate-runoffs-9-questions) there. A conservative local news network called Star News Group announced it would launch the Georgia Star in November, and NewsGuard’s analysis found that the website has published misleading information about the presidential election and the Senate races. One story making false claims about Georgia’s presidential election results reached up to 650,000 people on Facebook. Combating fake and misleading news would require efforts from multiple stakeholders. Yet Facebook [recently rolled back changes](https://www.nytimes.com/2020/12/16/technology/facebook-reverses-postelection-algorithm-changes-that-boosted-news-from-authoritative-sources.html) to its algorithm that would promote news from reliable sources. **Given the pace at which the problem is growing, the matter is likely to worsen without intervention.**

**Alliance Answers**

#### **Political problems threaten cohesion, undermine the plan’s effectiveness**

Psychogiou, Finabel researcher, ‘22

[Vasiliki Psychogiou, Finabel research intern, “Cyberspace: Is NATO Doing Enough?” Finabel—European Army Interoperability Centre, Info Flash, 2—22, p. 3]

Undoubtedly, cyberspace has become a key playing field of NATO’s overall defence and deterrence posture. Yet, the question remains whether the Alliance is doing enough. NATO’s internal challenges can significantly underestimate its efforts to build a solid cybersecurity posture. NATO has traditionally focused more on its military character rather than on its political role to promote constructive internal dialogue among its members, to consult on defence and security-related issues to solve problems, build trust and, in the long run, prevent conflict. Thus, it is essential that NATO updates its political foundation and enhances its political cohesion under its common purpose, that is, the protection of the Euro-Atlantic area (NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019).

Moreover, the Alliance has often been accused of being a monolithic structure rather than a hub of political dialogue (Shea, 2020). Disputes between its Allies have often impacted NATO unity on external matters. Driven mainly by national interests, these disputes have constrained NATO’s cohesion. Worries have also been expressed about the commitment of the United States to the defence of the European continent, the impact of the European Union’s development as a security actor on the future of NATO, the commitment of some European Allies to burden-sharing of defence, and the development of political inroads by NATO’s rivals into the Alliance territory (Reflection Group, 2020; Belkin, 2020; NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019; Shea, 2020). All these issues have significantly challenged NATO’s decision-making, which needs political cohesion to shape decisions, including on cyberspace-related matters.

#### **Unrelated disputes undermine the ability to generate consensus**

Lute & Burns, Harvard researchers, ‘19

[Ambassador Douglas Lute, Senior Fellow, Belfer Center and President, Cambridge Global Advisors and Ambassador Nicholas Burns, Professor, Diplomacy and International Politics, Harvard Kennedy School, “NATO at Seventy: An Alliance in Crisis,” Project on Europe and the Transatlantic Relationship, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2—19, p. 23]

A related problem is the tendency of some allies to bring into the Alliance bilateral issues that impede progress on collective issues of the Alliance. As an example, an ally might hold up agreement on the entire NATO military exercise program because of an unrelated bilateral dispute with a NATO partner who wishes to participate in an exercise.48 This practice erodes Alliance cohesion and should not be permitted. After appropriate consultation, we recommend the Secretary General should have the authority to exclude such external issues from consideration in the Alliance, even if it means moving forward without full consensus.

#### **Alliance Answers**

#### **Security cooperation now.**

Cho 4/14 (Han-Bum Cho, Senior Research Fellow, Unification Policy Research Division, “Evaluation of the Ukraine Crisis and Prospects on Changes in International Order”, https://210.117.224.39/bitstream/2015.oak/13221/1/CO22-10%28e%29\_수정본.pdf)

There is a possibility that a new global confrontation will emerge. The Biden administration has strengthened solidarity with the alliance and expanded cooperation with the democratic camp, including hosting the ‘World Democratic Summit.’ Due to the invasion of Ukraine, Russia is already defined as the "New Axis of Evil," dubbed by Biden. The Biden administration is expected to strengthen the cooperation system of the democratic camp in the wake of the Ukraine crisis to form a confrontational structure against authoritarian camps such as Russia and China. However, it is necessary to be careful in defining the global confrontation structure formed by the post-Ukraine situation as a new Cold War. In the case of the Cold War, the communist bloc formed its own regional value chain, such as COMECON, and was not highly dependent on the capitalist camp. On the other hand, Russia and China rely on the Global Value Chain. Strengthening the global solidarity of the democratic camp is also not an easy task in that the situation of democracy and human rights in each country can be widely different. However, given that most advanced capitalist countries are on democracy, the formation of a confrontation between the U.S.-led camps of democracy versus authoritarianism will be seen as a challenge for China and Russia. Strategic competition between the U.S. and China is likely to intensify. Despite the Ukraine crisis, the U.S. diplomatic and security posture of keeping China in check in the India-Pacific region has not changed much. In particular, NATO's rapid arms build-up may ease the burden on the U.S., which may boost its India-Pacific strategy. Given that the Ukraine crisis has strengthened NATO's unity, there is a possibility that the United States would use it to strengthen checks on China. European countries have shown differences in their positions in checking China, but a strong response is expected if China pursues a pro-Russian policy. The Ukraine crisis is likely to be a negative factor for China, which is facing strategic competition with the U.S.

#### No risk of aff offense – NATO has no legitimacy and causes instability.

Tony Cartalucci, 7-14-2022, "A US withdrawal from NATO would most benefit Americans," (Tony Cartalucci is a writer for SOTT) https://www.sott.net/article/405349-A-US-withdrawal-from-NATO-would-most-benefit-Americans

NATO atrocities including the bombing of civilians with manned aircraft and unmanned aerial vehicles (UAVs), torture, and other abuses have further tarnished NATO's reputation as well as consumed the political legitimacy of many individual NATO members involved.

The fact that the numerous goals NATO supposedly seeks to achieve in Afghanistan have gone unmet for now nearly two decades also undermines the legitimacy and credibility of NATO and its member states.

Another recent NATO action was in Libya in 2011. The destruction of Libya triggered a refugee tidal wave that swept Europe, compromising socioeconomic stability and domestic security within the very heart of NATO's supposed area of responsibility.

Libya itself has been reduced to a failed state where terrorism now runs rampant, threatening security across North Africa and serving as a springboard for militancy and terror both regionally and globally.

**Russia Answers**

#### **Cyberattacks are rarely acts of war – considering them as such undermines NATO’s efforts to deal with legitimate acts of violence**

**Blessing, 4/25** -- Blessing, J. (2022, April 25). *The Russian cyber threat is here to stay and NATO needs to understand it*. AEI. Retrieved June 16, 2022, from https://www.aei.org/op-eds/the-russian-cyber-threat-is-here-to-stay-and-nato-needs-to-understand-it/

Since the Russian invasion of [Ukraine](https://www.foxnews.com/category/world/conflicts/ukraine), the Biden administration has escalated warnings about likely Russian cyber-attacks on American infrastructure and business. More worrying still, cyber alarmists like Senate Intelligence Committee Chairman Mark Warner, D-Va., have suggested that cyber-attacks from the Kremlin could be acts of war that trigger NATO’s collective defense. This sky-is-falling delusion, particularly from leaders with access to [classified intelligence](https://www.foxnews.com/category/tech/topics/cia), is at best counterproductive and at worst dangerous. Cyber-attacks are rarely acts of war, and treating them as if they are undermines [NATO](https://www.foxnews.com/category/world/world-regions/europe)’s ability to deal with real threats short of cyber war. NATO has only invoked Article 5 – which triggers a collective response – once and that was after the 9/11 attacks. Cyber-attacks are unlikely to destroy buildings and kill thousands in an instant. While collective defense extends to cyberspace, few operations could realistically be a cause for war. This would include cyber-attacks resulting in death or damage like traditional military operations or coordinated assaults that take the power grid or entire economic sectors offline. These scenarios are unlikely though: such attacks require far too much time, funding, manpower, and control. Instead, most attacks temporarily overwhelm servers with traffic, deny network access, hold computers hostage, and steal or delete data. Even if allies wanted to trigger Article 5 over cyber operations, disagreements about the definitions of threats, origins of attacks, and pain thresholds in cyberspace can derail the process. Collective retaliation requires a unanimous vote across NATO; building unity across these points is nearly impossible for most cyber activity. Unlike missile attacks or tanks in the streets, few “red lines” exist to distinguish cybercrime, cyber espionage, and cyber disruption from digital acts of war. Beyond the bureaucratic and logistical limitations of elevating cyber to a casus belli, focusing on cyber-attacks as acts of war distracts from the more likely Russian digital assaults below the level of armed conflict. These include ransomware attacks and supply chain infiltrations that look like criminal activity or espionage. The Kremlin is particularly adept at the latter. In the SolarWinds compromise, Russia hacked one company’s software product to access networks of Fortune 500 companies and U.S. government agencies.

#### **Cyberattacks will not warrant and Article 5 response – NATO must build cyber resilience rather than preparing for “cyber doomsday”**

**Blessing, 4/25** -- Blessing, J. (2022, April 25). *The Russian cyber threat is here to stay and NATO needs to understand it*. AEI. Retrieved June 16, 2022, from https://www.aei.org/op-eds/the-russian-cyber-threat-is-here-to-stay-and-nato-needs-to-understand-it/

Spillover from operations in Ukraine poses an additional risk. The Russians have already deployed several digital tools to destroy computer data, resulting in corrupted computers for Ukrainian companies with government support roles. The same malicious software has also affected several Latvian and Lithuanian businesses. The danger is another situation like NotPetya in 2017, where malware self-replicated, spread past Ukrainian targets to cripple networks in over 150 countries, and created $10 billion in damages. Each of these scenarios are much more likely than a “cyber doomsday” that would justify an Article 5 response from NATO members. To be fair, policymakers’ fears of cyber war have led to some positive developments for the alliance. For instance, over the last several years, NATO has developed its own framework for combining cyber and conventional military capabilities in warfighting. But allies remain unprepared to deal with “death by 1000 cuts” in cyberspace. Concentrating only on acts of war comes at the expense of addressing the cumulative costs of low-level cyber threats over time. It leads to an overreliance on cyber deterrence or defensive whack-a-mole strategies, neither of which are sustainable. Threats of retaliation simply don’t deter most cyber-attacks, and it is unrealistic for defensive measures to stop every hacker. Policymakers across NATO must acknowledge that security failures are the norm in cyberspace, and that the compounding costs of failure over time are every bit as dangerous as the threat of cyber war. Building cyber resilience is an important step forward. It acknowledges that, in many cases, the Russians will get the best of us in cyberspace. The focus is on controlling failures to limit damage and quickly get networks back online. Moving from buzzword to actual strategy requires addressing several questions. Which digital assets are most significant? Where is the alliance most exposed to Russian cyber-attacks? Where should NATO reduce operating risks, and in what areas can it assume more? How can allies track long-term trends and adapt to new technologies? The Russian cyber threat is here to stay. Collective defense is – and should remain – the cornerstone of NATO. But time is running out for the alliance to protect itself from scenarios that aren’t all-out cyber war.

**Russia Answers**

#### **No nuclear retaliation**

Patrick Tucker 18, Technology Editor for Defense One, MA from Johns Hopkins University, BA from Sarah Lawrence College, Former Deputy Editor for The Futurist, “No, the US Won’t Respond to A Cyber Attack with Nukes”, Defense One, 2/2/2018, <https://www.defenseone.com/technology/2018/02/no-us-wont-respond-cyber-attack-nukes/145700/>

No, the US Won’t Respond to A Cyber Attack with Nukes

Defense leaders won’t completely rule out the possibility. But it’s a very, very, very remote possibility.

The idea that the U.S. is building new low-yield nuclear weapons to respond to a cyber attack is “not true,” military leaders told reporters in the runup to the Friday release of the new Nuclear Posture Review.

“The people who say we lowered the threshold for the use of nuclear weapons are saying, ‘but we want these low-yield nuclear weapons so that we can answer a cyber attack because we’re so bad at cyber security.’ That’s just fundamentally not true,” Gen. Paul Selva, vice chairman of the Joints Chiefs of Staff, said Tuesday at a meeting with reporters.

It’s an idea that military leaders have been pushing back against since the New York Times ran a Jan. 16 story headlined, “Pentagon Suggests Countering Devastating Cyberattacks With Nuclear Arms.”

When would the U.S. launch a nuclear attack in response to a non-nuclear event? The Defense Department says the threshold hasn’t changed since the Obama administration’s own nuclear posture review in 2010, but a draft of the new review that leaked online caused a bit of drama in its attempts to dispel “ambiguity.”

The new review gives examples of “non-nuclear strategic attacks,” Robert Soofer, deputy assistant secretary for nuclear and missile defense policy, told reporters on Thursday. “It could be catastrophic attacks against civilian populations, against infrastructure. It could be an attack using a non-nuclear weapon against our nuclear command-and-control [or] early-warning satellites. But we don’t talk about cyber.”

In his own conversation with reporters, Selva broadened “early warning” systems to include ones that provide “indications of warning that are important to our detection of an attack.” He also emphasized, “We never said ‘cyber.’”

There’s a reason for that. While cyber attacks on physical infrastructure can be very dangerous, they are unlikely to kill enough people to provoke a U.S. nuclear response.

An National Academies of Science and Engineering analysis of the vulnerability of U.S. infrastructure makes that point. A major cyber attack could cut off electrical power, resulting in “people dying from heat or cold exposure, etc.,” said Granger Morgan, co-director of the Carnegie Mellon Electricity Industry Center and one of the chairs of the report. “A large outage of long duration could cover many states and last for weeks or longer. Whether and how many casualties there could be would depend on things like what the weather was during the outage.”

It’s a huge problem but not an event resulting in tens of thousands of immediate deaths.

Contrast that with a nuclear attack on a city like Moscow, even one using a device of 6 kilotons, much smaller than the ones the United States used against Japanese targets in World War II. The immediate result: there would be 40,000 deaths, according to the online nuclear simulation tool NukeMap.

Russia has demonstrated a willingness to take down power services with cyber attacks, as they did in Ukraine on Christmas Eve 2015. But these attacks were brief and occured in the context of actual fighting.

In other words, the worst cyber physical attack that top experts believe credible likely does not meet the threshold that the Defense Department has set out for deploying a nuclear weapon.

#### **Cyber threat is overblown—Russian efforts against Ukraine prove**

Marschmeyer, CSS Senior Researcher and Kostyuk, Georgia Tech Assistant Professor, ‘22

[Lennart Maschmeyer, Senoir Researcher, Center for Security Studies, ETH Zurich and PhD, University of Toronto and Nadiya Kostyuk, Assistant Professor, School of Public Policy, Georgia Institute of Technology, “There Is No Cyber ‘Showck and Awe’: Plausible Threats in the Ukrainian Conflict,” WAR ON THE ROCKS, 2—8—22, <https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/>, accessed 5-11-22]

These predictions suggest that cyber operations will provide significant strategic advantages to Russia either as complements to military force, or as standalone instruments — or at least that policymakers and commentators think that they will. Current warnings of escalating cyber warfare conjure deep-seated fears of cyber doom and the recurring specter of a “cyber Pearl Harbor” strategic surprise attack. In practice, however, cyber warfare has been a failure. Our research shows that cyber operations have remained irrelevant on the battlefield, while standalone operations to weaken Ukraine through election interference, critical infrastructure sabotage, and economic disruption largely failed to contribute to Russia’s strategic goals of making Ukraine abandon its pro-European Union and pro-NATO foreign policy. Consequently, current fears of cyber warfare defy not only Russia’s track record in Ukraine, but also strategic logic. Given that Russia’s cyber operations have failed to produce significant strategic value to date, why would we expect this to suddenly change now? Or, to put it more pointedly: If cyber operations offer such effective and potent instruments, why did Russia go through the trouble (and costs) to mobilize its troops? Current predictions of cyber onslaught do not offer a persuasive answer.

Giving in to these fears risks fighting phantom threats, playing into Russia’s hands by distracting from the need to counter its military threat and sowing fear and confusion — at least among Western audiences. A level-headed analysis of the threat that distinguishes what is theoretically possible from what is practically feasible is urgently needed. Our research suggests that, contrary to hysteria, cyber operations will remain of secondary importance and at best provide marginal gains to Russia.

Expectations Versus Evidence: Cyber Operations and Their Limits

There are three distinct perspectives on the strategic role and value of cyber operations in conflict. Early scholarship on cyber conflict expected cyber operations to be primarily important in conventional military conflict, enabling crippling strategic strikes analogous to the surprise attack on Pearl Harbor during World War II. If successful, cyber operations could thus be substituted for the use of force. Yet research throughout the 2010s made the limitations of cyber operations as a means of force projection increasingly clear.

Subsequent scholarship thus sees cyber operations primarily as complements to force. Possible effects include disrupting command and control and communications systems, sabotaging equipment and infrastructure, spreading disinformation, and conducting psychological warfare to undermine morale among enemy troops.

The third and increasingly influential perspective instead suggests cyber operations are primarily relevant in “gray zone” conflict short of war. In this view, cyber operations offer standalone instruments of power that can influence and weaken an adversary through critical infrastructure sabotage, economic disruption, and influence operations. Hence, as in cyber Pearl Harbor scenarios, it also suggests that cyber operations could substitute for the use of force — achieving similar goals without going to war. However, rather than through a massive surprise strike, this third school of thought expects the effects to be gradual and cumulative, eroding adversary strength over multiple operations.

The empirical record of cyber conflict, however, suggests that what is feasible in practice is far more limited. Ukraine has been a “giant test lab” where Russia, one of the world’s foremost cyber powers, has experimented with cyber operations for eight years. Yet these operations have failed to produce significant strategic value either as force complements or standalone tools.

The substitutability argument — that states can or do substitute cyber operations for the use of force — has little empirical support since Russia levied no major cyber operations against Ukraine in the runup to the military escalation of the conflict in 2014. While it is possible that we do not know about such operations given their veil of secrecy, it is clear that any attempted but undetected cyber surprise strike failed to produce any measurable effects.

Evidence supporting the complementarity perspective is similarly sobering. One of us has examined the role of low-level disruptive cyber operations in the military conflict and their relevance for battlefield events (and outcomes). Disruptive attacks can directly affect military operations as they seek to sabotage an opponent’s ability to fight. For example, the Russia-backed separatists in the Donbas and Luhansk regions used malware to retrieve data from mobile devices on the locations of Ukrainian artillery troops, facilitating better reconnaissance against these troops. Pro-Ukrainian hackers hijacked CCTV cameras behind enemy lines to obtain intelligence on the movement of Russian artillery in the separatist-controlled territories.

Focusing on the period of the most intense fighting, between 2014 and 2016 — the time when, if cyber tools are an effective complement to armed force, Russia would have been most likely to use them — we applied a series of statistical tests to thousands of cyber and military operations. The findings showed a strong, escalatory dynamic between military operations by both sides but no significant correlation in either direction between military and cyber operations, and no reciprocity between cyber operations. This evidence demonstrates that in one of the first armed conflicts where both sides used low-level cyber operations extensively, digital operations unfolded independently from the events on the ground and had no discernible effect on them. Hence, in stark contrast to expectations about the force-multiplying advantages of cyber operations, these findings suggest hacking groups faced considerable difficulties in responding to battlefield events, much less shaping them.

Finally, the track record of cyber operations as standalone instruments in gray zone conflict in Ukraine also falls far short of expectations. One of us has examined the operational mechanisms, effects, and strategic value of five major Russia-sponsored cyber operations, including election interference, critical infrastructure sabotage, and economic disruption. Contrary to prevailing expectations, the majority made no measurable contribution towards Russia’s strategic goals. The NotPetya operation, whose large-scale disruption of businesses wiped off half a percentage point of Ukraine’s gross domestic product in 2017, is the exception. Yet this operation underlined a key shortcoming of cyber operations: the risk of losing control over the spread of effects, producing unintended consequences, added costs, and correspondingly lowering strategic value. Forensic analysis by internet security company ESET revealed that the Sandworm hacking group underestimated how far NotPetya’s data-destroying malware would spread. It “went out of control” and spread far beyond Ukraine, even disrupting targets in Russia — including the state-controlled oil giant Rosneft. These disruptions within Russia will have caused additional costs, as did the sanctions that Western countries imposed on Russia in response to NotPetya’s international disruption.

Evidence from Ukraine thus supports neither the force substitute nor the force complement argument. Instead, cyber operations have been most relevant as standalone, lower-intensity alternatives to the use of force — more in line with the third school of thought. Yet by and large they fell short of providing measurable strategic value. Indeed, all available evidence indicates that Russia’s cyber warfare efforts against Ukraine — combined with its larger gray zone campaign — have failed to make Ukraine abandon its rapprochement with the West. That is why Russia has mobilized its army, attempting to prevent Ukraine from joining the Western alliance through threat of invasion.

Plausible Threats in the Conflict Ahead

Considering the underwhelming track record of cyber warfare in Ukraine to date, there is little reason to expect cyber doom of the kind that some now predict. For these warnings of a Russian cyber onslaught to become reality, cyber operations would need to produce effects at a scope and scale that they have previously failed to attain. Importantly, current warnings fail to make a persuasive case on why we should expect such a transformation.

Rather, they rest on the implicit assumption that with the change in strategic context, the role of cyber operations will change as well. This comes out clearest in Maggie Miller’s recent commentary suggesting that military escalation in Ukraine would finally herald “a true cyberwar” where Russia could “take down the power grid” or launch a disinformation campaign to undermine the government in Kyiv. Dmitri Alperovitch offers a more level-headed analysis, underlining that cyber operations alone will fall short of achieving Russia’s goals. However, he also suggests that they can complement force as an “extension of warfare itself,” disrupting command and control to provide battlefield advantages, sabotaging critical infrastructure, and undermining public trust in the government to “send a powerful signal that resistance is futile.” Yet, as we have seen, Russia has attempted most of these objectives in the past and has failed. Even in a full-scale invasion, we have the same aggressor, with the same hacking groups, with the same skill level going after the same sets of possible targets. Why would we expect different results?

Changing the strategic context of deployment does not change the mechanism of action that cyber operations rely upon to produce outcomes — and its intrinsic constraints. Cyber operations rely on a mechanism of subversion that exploits vulnerabilities in adversary systems to use them against the adversary. This mechanism holds great strategic promise but poses significant operational challenges. It requires creativity and cunning to remotely manipulating complex systems that others designed and operate without alerting the victim to one’s presence. These challenges produce an operational trilemma between the speed, intensity of effects, and level of control that actors have over these effects. This trilemma limits strategic value, since in most circumstances cyber operations will be too slow, too weak, and too volatile to contribute measurably to strategic goals. The constraining role of this trilemma is evident across all five of Russia’s disruptive cyber operations against Ukraine thus far, underlining their relevance. Importantly, all available evidence indicates that these intrinsic constraints limit the strategic value of cyber operations regardless of strategic contexts.

**Russia Turn**

#### **As Russia feels threatened by the increasing NATO cooperation, they are increasingly likely to launch cyberattacks. The USFG and private sector cybersecurity firms are not prepared to face Russian attacks.**

O’Connor & Jamali, 2022. (Tom  an award-winning senior writer of foreign policy at Newsweek, Naveed a Newseek editor and former FBI double agent, January 24). Russia Could Launch Cyber Attacks Against U.S. if Biden Sends Wrong Signals, Intel Warns. Newsweek. <https://www.newsweek.com/russia-could-launch-cyber-attacks-against-us-if-biden-sends-wrong-signals-intel-warns-1672280>

Given past cyber-attacks Washington has attributed to Moscow and the current level of escalation, however, others emphasized a need to reinforce digital defenses.

"Russia has telegraphed that they are willing to attack critical infrastructure here in the U.S.," Brian Harrell, who served as former Department of Homeland Security Assistant Secretary for Infrastructure Protection before his resignation in August 2020, told Newsweek.

"The private sector should work to understand enemy tactics, including spear-phishing and brute force attacks while conducting proactive threat hunting efforts," he added. "We have absolutely entered a heightened period of awareness given the threats that have been made and the demonstrated attacks we've seen from the Russian GRU and Foreign Intelligence Service."

Kyiv has already accused Moscow of employing covert cyber tactics throughout the course of the current dispute, which first began to grab global attention in March of last year and then again in November as up to 100,000 Russian troops amassed near the country's restive border with Ukraine, where Russia-aligned separatists have been active since 2014. An apparent cyber-attack gripped the post-Soviet Eastern European state earlier this month, but Russian officials have dismissed any allegations their government was behind the incident.

In an interview with NBC News on Sunday, Secretary of State Antony Blinken warned that "in the event that there is a renewed Russian incursion, Russian forces going into Ukraine, there is going to be a swift, a severe, and united response" and also threatened such a reaction in response to other things "Russia could do short of sending forces into Ukraine again to try to destabilize or topple the government – cyber attacks, hybrid means, et cetera."

That same day, Peskov too criticized what he called "information hysteria" when it came to the situation between Russia and Ukraine. He placed the blame on the U.S. and NATO, however, and said Western powers were also responsible for real-world provocations as well. "As for concrete actions, we see the statements published by NATO about the increase of the contingent and relocations of forces and means to the eastern flank," Peskov said. "All this leads to an escalation of tensions."

#### **NATO expansion triggers Russian aggression.**

Bender, 2015, (Jermy, BA in Middle Eastern Studies, Fulbright Fellow), “This is the simplest explanation of why Putin is so opposed to NATO”. Business Insider. 02/12. <https://www.businessinsider.com/simplest-explanation-of-why-putin-hates-nato-2015-2>

Putin's suspicion of NATO can be boiled down to one simple explanation: geography. At the height of the Cold War and the Soviet Union's power, the USSR and its allied Warsaw Pact countries encompassed half of Europe and almost the entirety of Central Asia. But after the demise of the USSR in 1989, lands once within Moscow's orbit quickly peeled away to join NATO. Today, only Belarus remains firmly within Moscow's influence, and even that partnership has teetered recently. For Putin, the peeling away of countries from Russia towards NATO comes as both an existential threat and a personal insult. As a former agent in the KGB and an avowed nationalist, Putin has dreams of resurrecting the glories of Imperial Russia — a goal that is seriously hampered by the inclusion of what Putin would deem rightful Russian lands, such as the Baltics, into the NATO alliance. With this in mind, it is easy to see why Putin signed off on Russia's new military doctrine in December 2014. The doctrine, which placed explicit focus on NATO being Moscow's main existential enemy and threat, called on the further militarization of three geopolitical frontlines: the Russian Baltic Sea exclave of Kaliningrad near Poland, the annexed Crimean Peninsula, and the Arctic

#### **Russia Turn**

#### **Miscalculation risks triggering global nuclear conflict leading to mass death and extinction.**

Kallenborn, 2022, (Zachary, Research Affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), Policy Fellow at the Schar School of Policy and Government), “Giving an AI control of nuclear weapons: What could possibly go wrong?”. Bulletin of the Atomic Scientists. 02/01. <https://thebulletin.org/2022/02/giving-an-ai-control-of-nuclear-weapons-what-could-possibly-go-wrong/>

If artificial intelligences controlled nuclear weapons, all of us could be dead. That is no exaggeration. In 1983, Soviet Air Defense Forces Lieutenant Colonel Stanislav Petrov was monitoring nuclear early warning systems, when the computer concluded with the highest confidence that the United States had launched a nuclear war. But Petrov was doubtful: The computer estimated only a handful of nuclear weapons were incoming, when such a surprise attack would more plausibly entail an overwhelming first strike. He also didn’t trust the new launch detection system, and the radar system didn’t have corroborative evidence. Petrov decided the message was a false positive and did nothing. The computer was wrong; Petrov was right. The false signals came from the early warning system mistaking the sun’s reflection off the clouds for missiles. But if Petrov had been a machine, programmed to respond automatically when confidence was sufficiently high, that error would have started a nuclear war.

The huge problem with autonomous nuclear weapons, and really all autonomous weapons, is error. Machine learning-based artificial intelligences—the current AI vogue—rely on large amounts of data to perform a task. Google’s AlphaGo program beat the world’s greatest human go players, experts at the ancient Chinese game that’s even more complex than chess, by playing millions of games against itself to learn the game. For a constrained game like Go, that worked well. But in the real world, data may be biased or incomplete in all sorts of ways. For example, one hiring algorithm concluded being named Jared and playing high school lacrosse was the most reliable indicator of job performance, probably because it picked up on human biases in the data.

In a nuclear weapons context, a government may have little data about adversary military platforms; existing data may be structurally biased, by, for example, relying on satellite imagery; or data may not account for obvious, expected variations such as imagery in taken during foggy, rainy, or overcast weather.The deeper challenge is high false positive rates in predicting rare events. There have thankfully been only two nuclear attacks in history. An autonomous system designed to detect and retaliate against an incoming nuclear weapon, even if highly accurate, will frequently exhibit false positives.

In the extremely unlikely event those problems can all be solved, autonomous nuclear weapons introduce new risks of error and opportunities for bad actors to manipulate systems. Current AI is not only brittle; it’s easy to fool. A single pixel change is enough to convince an AI a stealth bomber is a dog. The decision to unleash nuclear force is the single most significant decision a leader can make. It commits a state to an existential conflict with millions—if not billions—of lives in the balance. Such a consequential, deeply human decision should never be made by a computer.

**NATO Overstretch Turn:**

#### **NATO’s focus on secondary issues from the Madrid Summit is key for preventing climate change, human trafficking, and ensuring security cooperation – the plan derails this focus by overstretching NATO**

**NATO 6/29** (North Atlantic Treaty Organization, “NATO 2022 Strategic Concept’’, <https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf>, NATO Madrid Summit, June 29, 2022); DOA: 7/13/22//KC

NATO’s enlargement has been a historic success. It has strengthened our Alliance, ensured the security of millions of European citizens and contributed to peace and stability in the Euro-Atlantic area. We reaffirm our Open Door policy, consistent with Article 10 of the North Atlantic Treaty, as an expression of our fundamental values and our strategic interest in Euro-Atlantic peace and stability. Our door remains open to all European democracies that share the values of our Alliance, which are willing and able to assume the responsibilities and obligations of membership, and whose membership contributes to our common security. Decisions on membership are taken by NATO Allies and no third party has a say in this process. 10 41. The security of countries aspiring to become members of the Alliance is intertwined with our own. We strongly support their independence, sovereignty and territorial integrity. We will strengthen political dialogue and cooperation with those who aim to join the Alliance, help strengthen their resilience against malign interference, build their capabilities, and enhance our practical support to advance their EuroAtlantic aspirations. We will continue to develop our partnerships with Bosnia and Herzegovina, Georgia and Ukraine to advance our common interest in Euro-Atlantic peace, stability and security. We reaffirm the decision we took at the 2008 Bucharest Summit and all subsequent decisions with respect to Georgia and Ukraine. 42. Political dialogue and practical cooperation with partners, based on mutual respect and benefit, contribute to stability beyond our borders, enhance our security at home and support NATO’s core tasks. Partnerships are crucial to protect the global commons, enhance our resilience and uphold the rules-based international order. 43. The European Union is a unique and essential partner for NATO. NATO Allies and EU members share the same values. NATO and the EU play complementary, coherent and mutually reinforcing roles in supporting international peace and security. On the basis of our longstanding cooperation, we will enhance the NATO-EU strategic partnership, strengthen political consultations and increase cooperation on issues of common interest, such as military mobility, resilience, the impact of climate change on security, emerging and disruptive technologies, human security, the Women, Peace and Security agenda, as well as countering cyber and hybrid threats and addressing the systemic challenges posed by the PRC to Euro-Atlantic security. For the development of the strategic partnership between NATO and the EU, nonEU Allies’ fullest involvement in EU defence efforts is essential. NATO recognises the value of a stronger and more capable European defence that contributes positively to transatlantic and global security and is complementary to, and interoperable with NATO. Initiatives to increase defence spending and develop coherent, mutually reinforcing capabilities, while avoiding unnecessary duplications, are key to our joint efforts to make the Euro-Atlantic area safer. 44. We will strengthen our ties with partners that share the Alliance’s values and interest in upholding the rules-based international order. We will enhance dialogue and cooperation to defend that order, uphold our values and protect the systems, standards and technologies on which they depend. We will increase outreach to countries in our broader neighbourhood and across the globe and remain open to engagement with any country or organisation, when doing so could bolster our mutual security. Our approach will remain interest-driven, flexible, focused on addressing shared threats and challenges, and able to adapt to changing geopolitical realities. 11 45. The Western Balkans and the Black Sea region are of strategic importance for the Alliance. We will continue to support the Euro-Atlantic aspirations of interested countries in these regions. We will enhance efforts to bolster their capabilities to address the distinct threats and challenges they face and boost their resilience against malign third-party interference and coercion. We will work with partners to tackle shared security threats and challenges in regions of strategic interest to the Alliance, including the Middle East and North Africa and the Sahel regions. The Indo-Pacific is important for NATO, given that developments in that region can directly affect EuroAtlantic security. We will strengthen dialogue and cooperation with new and existing partners in the Indo-Pacific to tackle cross-regional challenges and shared security interests. 46. NATO should become the leading international organisation when it comes to understanding and adapting to the impact of climate change on security. The Alliance will lead efforts to assess the impact of climate change on defence and security and address those challenges. We will contribute to combatting climate change by reducing greenhouse gas emissions, improving energy efficiency, investing in the transition to clean energy sources and leveraging green technologies, while ensuring military effectiveness and a credible deterrence and defence posture.

#### **NATO drafts its strategic concepts with limited resources in mind. There is only room to reduce not increase responsibilities.**

US Senate 9. "NATO: A Strategic Concept For Transatlantic Security." Committee on Foreign Relations United States Senate. 10-22-2009. https://www.govinfo.gov/content/pkg/CHRG-111shrg56689/html/CHRG-111shrg56689.htm. //AN

As NATO leaders draft a new strategic concept, they will also need to consider political and military reforms to ensure that the commitments made at next year's Lisbon summit can be implemented. Such reforms will be critical in light of the limited financial and human resources that are likely to be available to the alliance in coming years. At this early stage in the work of the Group of Experts, it would be premature to pronounce on the specific reforms and implementation plans that should be considered. There can be no doubt, however, that there is room to improve the efficiency of NATO

decision making and the effectiveness of alliance expenditures.

**NATO Overstretch Turn:**

#### **Climate remains high priority post-Ukraine.**

Kirton & Warren, 3/22 – professor of political science and the director and co-founder of the G7 Research Group, co-director and founder of the G20 Research Group (John Kirton and Brittaney Warre; "Will the War in Ukraine Crowd Out G7 Climate Action in 2022?"; G7 Information Center; http://www.g7.utoronto.ca/evaluations/2022elmau/kirton-warren-ukraine-crowd-out.html; 3-22-2022, Accessed 6-24-2022)//ILake-NoC

G7 Performance on Security and Sustainability on March 10 and 11

The Ukraine crisis could still easily derail the G7's climate-focused agenda. And there are signs it has done so to some extent. On March 11, G7 leaders released a statement focused solely on Ukraine. It therefore did not mention climate change at all (see Appendix B-1). It did make two energy commitments, but neither spoke of a clean energy transition (see Appendix B-2). However, the G7's energy ministers, who met on March 10, the day before their leaders, made a clean energy transition a high priority in their own statement on Ukraine. The G7 energy ministers stated: "We remain steadfastly committed and convinced that the most important contribution towards energy security is an accelerated clean energy transition based on energy efficiency and a shift to the use of clean, safe and sustainable energies." Of their 13 commitments, nine (69%) explicitly referenced clean energy, the energy transition, climate change or the Paris Agreement (see Appendix C). Although the following day the agriculture ministers put less emphasis on climate change, two of their 15 commitments, for 13%, committed to support food security in line with climate, environment and sustainable development commitments (see Appendix D). This suggests that the Ukraine crisis will not totally overshadow climate governance before or at Elmau.

#### **Unchecked climate change causes extinction.**

Jeff Master 21. Ph.D., is a former hurricane hunter and scientist for the National Oceanic and Atmospheric Administration (NOAA), as well as the co-founder of Weather Underground. He writes about extreme weather and climate change for Yale Climate Connections. “How easily the climate crisis can become global chaos” The Hill. 09-01-21. https://thehill.com/opinion/energy-environment/570284-how-easily-the-climate-crisis-can-become-global-chaos?amp

After months of one extreme weather event after another, it's hard to imagine how climate impacts could get any worse. Unfortunately, it could. Imagine a year - **not far in the future** - just a couple years from now, where it all goes wrong: A strong El Niño event warms the equatorial Pacific, bringing Earth's hottest January on record. Extreme drought grips Australia, the world's No. 3 exporter of wheat, bringing its most intense drought in history. A 58 **percent decline in wheat production** results, as occurred after their 2002 drought. **Global food prices spike.** In April, record rainfall hits Canada, the world's No. 2 wheat exporter. Canada's wheat harvest falls 14 percent, as occurred after extreme rains in 2010. Unrelenting torrential rains hit the central U.S., delaying spring planting of crops and bringing near-record flooding on the Mississippi and Missouri rivers. Fortunately, because of infrastructure bills passed in 2021 and 2022, which gave funds for flood preparedness, the damage is billions of dollars less than from the great floods of 2011 and 1993. As summer arrives, the jet stream gets "stuck" in the type of resonant pattern linked to human-caused climate change that has become more frequent in recent years. The stuck jet stream brings cool air, relentless rain-bearing low-pressure systems and record rains to the central United States. Production of corn falls 4 percent and wheat 25 percent, as occurred in 2017 after a similarly wet year. In the western U.S. and Canada, the stuck jet stream brings a **record-strength dome of high pressure**, exacerbating their intense drought and bringing another year of **hellacious wildfires and choking smoke** that leads to thousands of premature air pollution deaths. Severe drought, typical of an El Niño year, hits India and Southeast Asia, causing failure of the monsoon rains. In India, "Day Zero" arrives for an additional 100 million people, as taps run dry from years of excessive groundwater pumping and a wasteful water supply system. Rice yields fall 23 percent in India, the world's No. 1 rice exporter, as occurred in 2002. In the fall, another bonkers Atlantic hurricane season unfolds as record-warm waters in the Caribbean fuel five major hurricanes, bucking the tendency of El Niño to suppress hurricanes. In mid-October, a hurricane - a carbon copy of 2021's Hurricane Ida, except occurring during peak harvest season - trashes three of America's 15 largest ports, which lie along the Lower Mississippi River and handle 60 percent of all U.S. grain exports to the world. Barge traffic on the Mississippi is crippled for months, during the peak export period for U.S. grain. The extreme weather **onslaught causes food prices** to spike to quadruple the levels of 2000. **Food riots break out** in urban areas across the Middle East, North Africa and Latin America. The Euro weakens and the main European stock markets lose 10 percent of their value; U.S. stock markets fall 5 percent. **Civil war erupts** in Nigeria, **famine kills nearly a million** people in Bangladesh and Africa, and Mali becomes a failed state. **Military tensions heighten** between Russia and NATO; **nuclear-armed India and Pakistan fight** a border skirmish over water rights. Even more dramatic stock market falls ensue, and the **global economy tumbles into a deep recession.** This worst-case scenario year - though unlikely to occur exactly this way - illustrates one of the greatest threats of climate change: **extreme droughts and floods** hitting multiple major grain-producing "breadbaskets" simultaneously. The scenario is similar to one outlined by insurance giant Lloyds of London in a "Food System Shock" report issued in 2015. Lloyds gave uncomfortably high odds of such an event occurring - well over 0.5 percent per year, or more than an 18 percent chance over a 40-year period. Given the unprecedented weather extremes that have rocked the world recently, the odds of a devastating food system shock are probably **much higher**. What's more, these odds are steadily **increasing as humans burn fossil fuels and pump more heat-trapping greenhouse gases into the air.** A warming planet provides more **energy to power stronger storms**, and more energy to intensify droughts, heatwaves and wildfires when storms are not present. Earth's **oceans are heating at an accelerating rate,** storing energy equivalent to an astonishing three to six Hiroshima-sized atom bombs per second. That extra heat energy allows more water vapor to evaporate and power stronger and wetter storms - like Hurricane Ida, and the catastrophic storms that hit Europe and China in July, costing over $25 billion each. Earth's extra heat energy also intensifies droughts and heatwaves, like the one that brought Canada's all-time heat record in June: 121 degrees Fahrenheit in Lytton, British Columbia, a day before a wildfire burned the town down. Global warming also intensified the 2010 Russian drought, which caused a doubling in global wheat prices, helping fuel the Arab Spring protests that led to the deadly uprisings in seven nations and the overthrow of multiple governments. If business-as-usual is allowed to continue, **a civilization-threatening climate catastrophe will occur.** Mother Nature's primal fury of 2021 is just a preview of what is coming. Global temperatures are currently about 1.2 degrees Celsius (2.2 degrees Fahrenheit) warmer than pre-industrial levels, and this year may well be the coolest year of the rest of our lives. Catastrophic extreme weather events will **grow exponentially worse** with 3 degrees Celsius of warming - **the course we are currently on.**