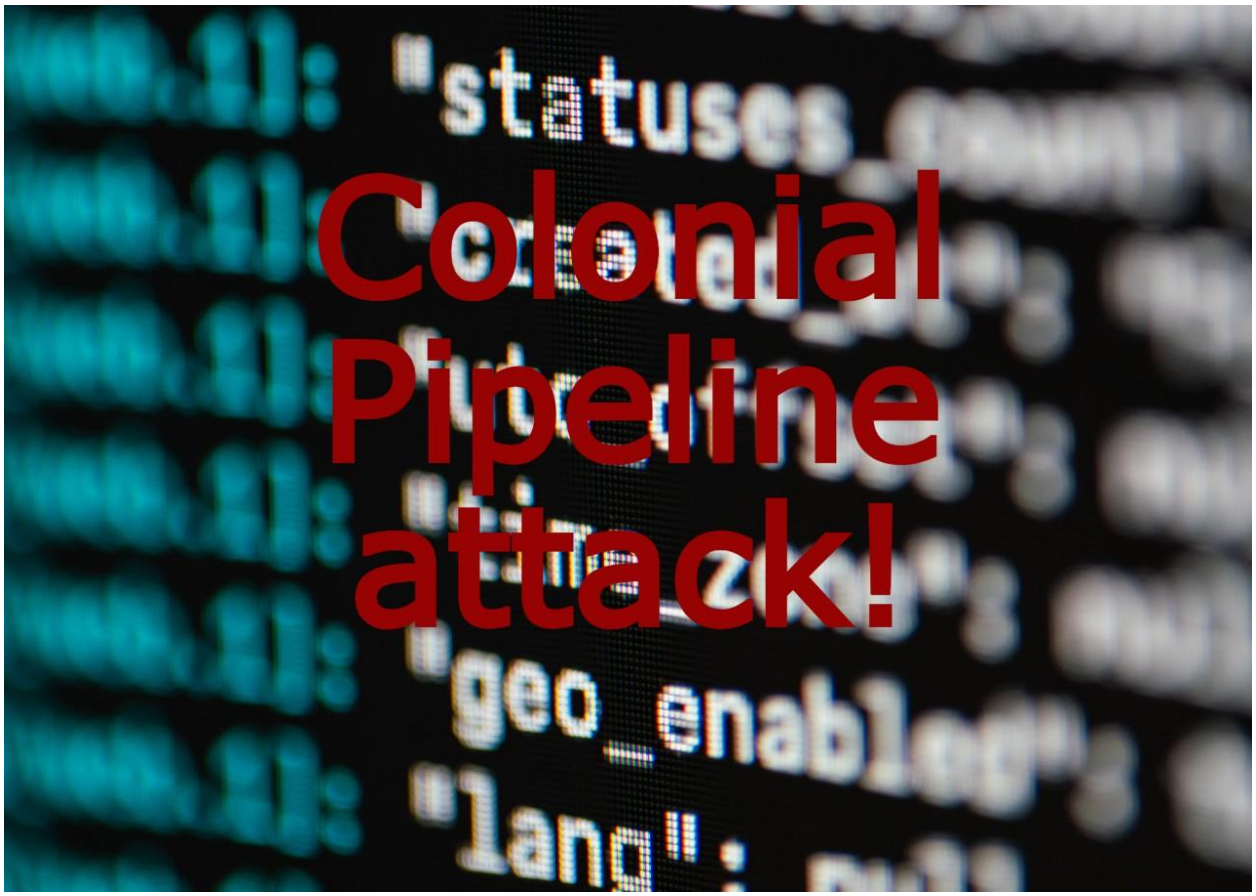
Colonial Pipeline attack: *a turning point for cyber norms?*

By Jennifer Korn



Will the ransomware attack on Colonial Pipeline change the international norms currently in place regarding nation-states and their historical hesitancy to engage in crippling infrastructure attacks? In this paper, we will explore some underlying issues and identify indicators of change which could help to evaluate potentially evolving norms.

Introduction:

It remains to be seen whether the Colonial Pipeline attack by DarkSide will unleash the monster that could become normalized state-sponsored infrastructure cyber sabotage and/or ransomware, but let us all acknowledge a few facts:

First: Nations are capable of attacking other countries' critical infrastructure. Examples include situations of measured retaliation, calibrated threat removal or selected messaging, as well as when powerful hegemons take less restricted actions within their region of influence or control to intimidate others.

Second: Most countries have thus far shied away from attacking critical infrastructure of other countries for fear of facing acts of retaliation against their own infrastructure systems and/or becoming the focus of international scrutiny. While selected acts of state-sponsored cyber sabotage have been considered somewhat justifiable when the attack is carefully gauged to retaliate, remove a threat or send a message in a way that is both deniable and falls short of war, other acts of cyber sabotage by regional hegemons which may be less justifiable have been less challenged due to geopolitical realities. However, state-sponsored ransomware attacks have been generally condemned as indiscriminate and money-grubbing.

Third: The Colonial Pipeline attack was massive in terms of how many people it disrupted, how large of a region was impacted, and how much media/government attention it received.

Last: Russia, China, Iran, the US and many others are in a cycle of cyber escalation. This is evident with the Solar Winds attack and the Microsoft Exchange hack, election manipulation, IP theft and more. Cyber espionage, cyber sabotage and ransomware are different types of actions, yet they exist along a blurry line and can all be applied to critical infrastructure.

Will these factors come together into the perfect storm? Are we entering into an age where China will turn your power off or Russia will shut down bridges and tunnels, either through cyber sabotage or ransomware?

State Due Diligence Responsibilities:

The Colonial Pipeline attack was carried out by DarkSide, a private ransomware-as-a-service company from Eastern Europe that targeted Colonial Pipeline for what they claimed to be apolitical, economic reasons. Colonial Pipeline ended up paying ransom money to DarkSide against FBI recommendations.

While President Biden articulated that the attack was not carried out by the Russian government, it was, "in Russia. They have some responsibility to deal with this."[1] The responsibility of states to police what their citizens do within and outside their borders is an international norm, yet some nations (such as Russia) look the other way when it suits them. By placing some blame on the Russian government for this attack, President Biden is suggesting that country versus country infrastructure attacks are moving closer to reality. While DarkSide and Colonial Pipeline are private entities, it is undeniable that the attack had a very public impact. Will this act push governments to begin engaging directly in infrastructure attacks, a line that traditionally has not been overtly crossed?

This due diligence norm applies in the cyber realm. The Tallinn Manual was published in 2013 and outlines how international law applies in the cyber realm. Though it is not binding, it is a highly respected and followed guide.[2] Section 2, Rule 6 of the Tallinn Manual explains that, "[a] state bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation," (29).[3] This could be in the form of an act or an omission. In the case of ignored attacks on infrastructure by actors within a national border, a country is committing an omission or failure to act. The due diligence principle says that if a state knows harm is coming from within its boundaries against people in another nation, that government has a responsibility to investigate and stop its citizens from committing harmful acts.[4]

[1] https://www.ttnews.com/articles/biden-says-russia-has-some-responsibility-colonial-attack
[2]https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE
[3] https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf
[4] https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

Underlying assumptions:

To consider how the Colonial Pipeline attack may or may not change global norms in terms of how willing or reluctant states are to practice sabotage and/or ransomware outside their regions of control, we must first make clear two underlying assumptions.

Assumption 1: The Colonial Pipeline attack has made the political impact of such a critical infrastructure attack much more visible. It may thus have a chain reaction and impact future norms.

Assumption 2: States have demonstrated the ability to attack critical infrastructure for sabotage AND ransomware and have been willing to do so in selected situations depending on how they gauge their own interests and possible responses.

“

Given these assumptions, is the Colonial Pipeline attack going to unleash/change the norm that makes most states reluctant to practice sabotage or ransomware? Especially, might locally hegemonic states be more willing to extend such attacks outside of their regions of influence/control?

”

Understanding Ransomware versus Sabotage:

First we must ask: what is ransomware? CISA defines it as an "ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable," used by malicious actors to extract ransom money from victims.[5] There is a ransomware attack on a business about every 11 seconds, and Cybersecurity Ventures predicts that such crimes cost over $6 trillion dollars annually.[6] Essentially, ransomware holds computer systems and sensitive information hostage, and routinely impacts real-world operations run by those systems. As this paper is being written, ransomware is evolving to taking and encrypting files, leaking information to extort victims, and holding systems hostage.

Private sector cyber attacks: Historically, ransomware has been used as a tool by private-sector hacking groups for a variety of reasons. The first known ransomware attack, AIDS Trojan, was in 1989 by Joseph Popp, PhD., against AIDS researchers across the world via floppy discs containing malware with the goal of extracting ransom money from victims.[7] However, because ransoms were to be mailed to a P.O. box in Panama, Popp didn't receive a high return for his efforts. But thirty one years later, at least 2,354 US-based organizations faced ransomware attacks in 2020, with at least $920 million paid in ransom to hackers in 2020 alone.[8]

State sponsored cyber attacks: There have also been incidents of ransomware attacks attributed to state sponsors for the sake of money or political messaging, such as WannaCry by North Korea and NotPetya from Russia in 2017. North Korea conducted the WannaCry attack against thousands of computers across 150 countries, infecting businesses, banks, hospitals and schools and demanding payment which would likely have supported the North Korean Government had the attack not been quickly thwarted.[9] NotPeyta appears to have been used by the Russians to send a clear message to Ukraine and perhaps to the rest of the world about doing business in Ukraine. As Andy Greenberg wrote in his book, *Sandworm,* "Ukraine has been locked in a grinding, undeclared war with Russia that has

[5] https://www.cisa.gov/ransomware
[6]https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
[7]https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#2
[8] https://www.motherjones.com/politics/2021/05/ransomware-colonial-pipeline/
[9] https://www.vox.com/world/2017/12/19/16794970/wannacry-north-korea-bossert-cyberattacks

killed more than 10,000 Ukrainians and displaced millions more. The conflict has also seen Ukraine become a scorched-earth testing ground for Russian cyberwar tactics. In 2015 and 2016, while the Kremlin-linked hackers known as Fancy Bear were busy breaking into the US Democratic National Committee's servers, another group of agents known as Sandworm was hacking into dozens of Ukrainian governmental organisations and companies. They penetrated the networks of victims ranging from media outlets to railway firms, detonating logic bombs that destroyed terabytes of data."[10] NotPetya was clearly a ransomware attack by a hegemonic government against an inferior power within its region of influence used to display dominance. Whether or not NotPetya might qualify as an act that crossed the threshold of war, ultimately, nations were willing to do little but scold Russia, while private companies absorbed the damages.[11]

Examples of nation-states engaging in infrastructure sabotage attacks via state-sponsored hacker groups in areas where they are clearly hegemonic also exist. One example is the 2015 attack on Ukraine's power grid by Russian military intelligence, the GRU. This attack falls into the same geopolitical context as the NotPetya attack described above. Another example is China's attack on India's power grid in 2020 when Chinese and Indian forces fought in the Galwan Valley border region. Four months later, Mumbai saw its power go out, wreaking havoc from trains shutting down to the stock market being forced to close. As the physical battle went on at the border, Chinese malware was working its way into the Indian electric control systems.[12] China engaged in infrastructure sabotage as a means of signaling to an inferior power, India, that it needed to stand down. While these acts are flexing of power by regional hegemons in situations over which the world may have limited geopolitical influence to respond, they signal Russian and Chinese ability and willingness to attack critical infrastructure-- a fact that could someday soon directly impact the US if global norms are changing.

Responses: Currently, government actions to combat ransomware against critical infrastructure are more focused on private companies than states. In a press briefing after the Colonial Pipeline attack, Deputy National Security Advisor for Cyber and Emerging Technologies Anne Neuberger said the United States is "pursuing greater international cooperation — ransomware affects countries around the world — to address ransomware

[10]https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html
[11] Greenberg, Andy, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History* (Wired, 22 August 2018), retrieved 14 June 2021
[12] https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html

because transnational criminals are most often the perpetrators of these crimes and they often leverage global infrastructure and global money-laundering networks." We should watch how states respond to America's request for greater international cooperation, since that will serve as one indicator of evolving norms.

The Darkside attack on Colonial Pipeline left a pipeline that brings gas to the entire east coast of the United States shut down for several days. While this act may seem extremely political-- especially coming from a criminal group in Eastern Europe, in and around the Russian sphere of influence-- DarkSide said in a statement, "[w]e are apolitical, we do not participate in geopolitics, do not need to tie us with a defined [government] and look for other our motives. Our goal is to make money, and not creating [sic] problems for society."[13]

Just how vulnerable is US critical infrastructure? If this attack reveals anything, it is that the answer to that question is *very*. While initially DarkSide claimed to have removed the ransomware due to US pressure, it was revealed that Colonial Pipelines paid off the ransom of 4.4 million dollars in bitcoin- though the FBI has now recovered about half of that.[14] This attack highlights the fact that there are no mandatory cybersecurity requirements for companies running US critical infrastructure. There are federal guidelines, but, since many pieces of infrastructure such as the pipeline are privately held, there is no obligation for companies to adhere to government advice in the cyber sphere. The national fall out-- regional state of emergency, gas shortages, widespread panic-- make it clear that private pieces of critical infrastructure and their cybersecurity measures, or lack thereof, are a national security issue.

[13] https://www.washingtonpost.com/technology/2021/05/14/darkside-ransomware-shutting-down/
[14]https://www.natlawreview.com/article/colonial-pays-millions-ransomware-attack-pipeline

State and private criminal relations:

Ransomware attacks on infrastructure have traditionally --with some exceptions explained above-- come from private cyber-criminal organizations. While private, however, they are often operating from "safe havens," nations where governments are unwilling or unable to properly investigate the crimes.[15] Russia is one such place where hackers have been able to flourish as long as they do not attack the Russian government. There are also cases where the Russians use the criminal's expertise for state intelligence purposes and allow them to steal on the side for profit. Examples include Maksim Yakubets and Igor Turachev, two cyberhackers who spent decades stealing from businesses around the world[16] and would also inform one of Russia's leading intelligence organizations, the FSB, on information they stole.[17] Russian hackers also got into Yahoo systems in 2014 and stole data, and, in 2017, the US Justice Department charged two Russian intelligence officers with the crime.[18] These examples show the blurry lines that exist between private crime and state-sponsored actions, and indicate how state-run cybercrime plays into the future of cyber conflict.

Indicators for the future:

There are several indicators that we should look at when gauging whether or not the norms about state-sponsored infrastructure sabotage or ransomware are changing. These include:

1) A rise over time in cybercriminals targeting critical infrastructure with ransomware.
2) Reaction of selected states to local cybercriminals who attack critical infrastructure: either reluctance or willingness to punish.
3) The actions of criminal groups such as DarkSide post-infrastructure attack.
4) A rise in state-run sabotage or ransom incidents in regions where powerful countries are hegemonic and can afford to wreak havoc without fear of dramatic retaliation and a rise in cybertensions.
5) If countries engage in ransomware or sabotage against critical infrastructure in areas where they are not hegemonic and/or not fearful of retaliation.
6) A rise in countries engaging in ransomware attacks just for money.

[15]https://www.pbs.org/newshour/show/what-does-the-colonial-pipeline-hack-tell-us-about-the-security-of-u-s-infrastructure
[16]https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens
[17] https://www.wired.com/story/alleged-russian-hacker-evil-corp-indicted/
[18] https://www.nytimes.com/2017/03/15/technology/yahoo-hack-indictment.html

Testing the indicators

Focusing on indicator 1, it is undeniable that nation-state-backed cyberattacks have grown in prominence over the last several years. The study *Nation States, CyberConflict and the Web of Profit* looked at over 200 cybersecurity breaches since 2009 and found that 40% of all incidents analyzed involved a physical infrastructure element as part of "hybridization," situations that include something like hitting a power plant with malware. Of the known targets of nation state cyber activity (which may include espionage, sabotage and ransomware), 10% of targets are critical infrastructure. In a 2019 survey of security staff in the utility, energy, health and transport sectors, 90% reported that there had been at least one attack successfully carried out on their systems between 2017 and 2019.[19]

Discussing indicator 2, we should also focus on the case of Colonial Pipeline. After the pipeline paid DarkSide millions in ransom, the US Department of Justice recovered a large portion of the money paid. The recovery operation to reclaim the cryptocurrency payment is the first of its kind in that it was successfully undertaken by a specialized ransomware task force. Deputy Attorney General Lisa Monaco said at a news conference that, "[b]y going after the entire ecosystem that fuels ransomware and digital extortion attacks -- including criminal proceeds in the form of digital currency -- we will continue to use all of our resources to increase the cost and consequences of ransomware and other cyber-based attacks," indicating the United States is willing and able to chase down cybercriminals who attack critical infrastructure.[20] However, the government is reluctant to punish Russia in any real way for allowing this kind of attack to happen, despite the hacking group likely originating there.

Another hopeful sign for indicator 2 are the cases of NetWalker and Emotet. The US worked with Canada, France, Germany, the Netherlands, the United Kingdom, Lithuania, Sweden, and Ukraine to disrupt the Emotet cybercrime ring using the European Multidisciplinary Platform Against Criminal Threats (EMPACT).[21] The US also seized hundreds of thousands of dollars from the NetWalker ransomware gang with the help of partnership with private entities and working with the Bulgarian government; the Bulgarian authorities seized the

[19] https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf

[20] https://apnews.com/article/technology-business-government-and-politics-8e7f5b297012333480d5e9153f40bd52

[21] https://www.europol.europa.eu/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action

dark web hidden resource.[22] This kind of international, cross-sector coordination is a positive sign for the future of the global fight against ransomware and cybercrime.

Indicator 3: The actions of DarkSide can be used to give some guidance for indicator 3. After the attack on Colonial Pipeline, the group claimed they would better vet their clients using their ransomware-as-a-service to avoid the kind of massive political impact of the Colonial pipeline attack.[23] However, just a week later, Russian cybercrime gang REvil attacked Brazil's JBS SA, the largest meat processing company in the world, impacting production and causing a chain reaction that impacted markets around the globe.[24] All of their US and Australia beef plants were forced to shut down, as well as one of the largest in Canada, and JBS ended up paying 11 million dollars to hackers.[25] How Brazil handles the situation on a governmental level remains to be seen and may provide more data for indicator 2. But REvil and DarkSide are apparently related,[26] so whether DarkSide had no control over the attack, decided that JBS was an appropriate target, or simply did not bother to vet the new target is still an open question.

President Biden and Vladamir Putin met at a summit in Switzerland in June 2021 and discussed global cybersecurity norms, bringing us to indicators 4 and 5. Biden told Putin that the US will not hesitate to use retaliation measures against Russia and criminal hacker groups originating from Russia targeting US critical infrastructure. Both sides agreed that experts from both nations will meet to write out explicit guidelines. However, it is unclear whether Russia will actually keep its word or if the US is actually willing to retaliate if they do not. Some experts believe words alone will not fix this, and perhaps the US will have to launch aggressive cyberattacks against Russia to make any real progress.[27] They argue that if Russia were to truly follow their word in establishing new cyber norms that protect critical infrastructure and punish hackers, they would no longer allow ransomware cybercriminal gangs to operate from the country and could even move towards extraditing criminals who broke the law. When Putin has been asked about the issue, he denies it: "I do hope that people would realize that there hasn't been any malicious Russian activity

[22] https://www.jdsupra.com/legalnews/u-s-takes-part-in-multinational-efforts-7907078/
[23]https://www.bleepingcomputer.com/news/security/darkside-ransomware-will-now-vet-targets-after-pipeline-cyberattack/
[24]https://apnews.com/article/technology-business-government-and-politics-8e7f5b297012333480d5e9153f40bd52
[25] https://www.nytimes.com/2021/06/09/business/jbs-cyberattack-ransom.html
[26] https://www.nytimes.com/2021/06/09/business/jbs-cyberattack-ransom.html
[27]https://www.washingtonpost.com/politics/2021/06/17/cybersecurity-202-here-are-four-cyber-takeaways-biden-putin-summit/

whatsoever," Putin said at an economic forum in St. Petersburg recently.[28] There seems to be little hope that Russia will change its behavior unless the US takes a more aggressive approach to punishing them for violating cyber norms.

It can be very difficult to assess indicators 4, 5 and 6 because the world of cyber conflict is one in which attribution is often difficult, and, for that reason, it is unclear how far we have already entered into a world in which critical infrastructure is under attack by foreign governments for simple profit, espionage, sabotage or preparation of the battlefield for future war. For example, in 2018, the United States accused Russia of conducting a cyber-intrusion campaign in the US power grid. The Department of Homeland Security and FBI said Russian government actors had targeted small commercial energy facilities, ""where they staged malware, conducted spear phishing, and gained remote access into energy sector networks."[29] Do these actions indicate a future where Russia shuts down our power system? If Russia converts the access gained through 2018 espionage to future sabotage of U.S. critical infrastructure as they did in Ukraine, it would be a shift in global norms, as this would be a clear instance of a nation attacking another nation's critical infrastructure without hegemony and with a true risk of retaliation.

In June 2021, we learned that the New York MTA was breached by Chinese state-linked hackers. While the hackers did not take control of the train cars or cause any damage, the attack is evidence that China is testing its capabilities to access and potentially affect the transit system of New York City.[30] If China were to move from access to sabotage or an act of ransomware, this would also point to indicator 5, a sign that the global norms on infrastructure attacks have changed.

Turning finally to indicator 6, if more states begin to engage in ransomware attacks on critical infrastructure (either government-sanctioned or perpetrated), it would be an indicator that the norms are shifting. For example, Iranian hackers have been holding data hostage from Israeli companies, demanding hundreds of thousands of dollars in bitcoin payment as a ransom. While these acts are attributed by the Iranian government as acts of "hacktivism" by Iranian individuals, they are also a monetary move against a nation over

[28]https://www.washingtonpost.com/politics/2021/06/14/cybersecurity-202-russia-agrees-cyber-rules-violates-them-same-time/
[29]https://www.reuters.com/article/us-usa-russia-sanctions-energygrid/in-a-first-u-s-blames-russia-for-cyber-attacks-on-energy-grid-idUSKCN1GR2G3
[30] https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html

which they do not have hegemony.[31] While Iran might be willing to take a page from the North Korean book and move to direct cyber theft from the international banking system to bypass sanctions, a more subtle step could be moving up from the relatively unsophisticated DDoS attacks featured in Operation Ababil in 2012 against the U.S. banking sector to ransomware against the financial or other critical infrastructure systems, Although the claimed attackers in Operation Ababil were independent hackers, they have since been tied to the Iranian state in a DoJ indictment.[32] In order to continue to monitor this indicator, we must watch for nations or their proxies beginning to engage in large-scale ransomware.

Why would countries *not* begin attacking critical infrastructure via cyber methods such as ransomware? A shift in global norms on this issue could be mutually catastrophic for all nations involved. As we analyze unfolding attacks, we can apply the above indicators to help us understand whether or not these global norms are changing. Understanding potentially changing norms will illuminate the attacks we may be facing in the near future and inform the US in how to shift its approach to respond to or try to get unleashed harmful norms back under control.

The FBI and DOJ have now elevated the priority of ransomware attacks to equal those of terrorist attacks. The public sector and private sector is at risk, and our entire infrastructure system- as well as the systems of countries across the globe- is at risk. Tracking and responding to potentially changing norms can help mitigate this risk.

[31]https://www.cpomagazine.com/cyber-security/suspected-iranian-ransomware-gang-n3tw0rm-starts-another-cyber-attack-wave-against-israel/
[32]https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

"

The public sector and private sector is at risk, and our entire infrastructure system- as well as the systems of countries across the globe- is at risk. Tracking and responding to potentially changing norms can help mitigate this risk.

"

The Global Techno Politics Forum is an innovative new organization that strives to shape the public debate and facilitate global coordination at the intersection of technology and geopolitics. The Forum is independent and nonpartisan, and the analyses and suggestions in this paper are the authors' alone. Yet, the Forum's work is very much that of the team, and we salute the entire team for this effort.

Gregory Treverton ***Pari Esfandiari*** ***Maura Godinez***

Chairman ***President*** ***Senior Director of Programs & Studies***