CYBERWAR WHITE PAPER

Understanding the Crisis and Opportunity

CYBER CAPITAL PARTNERS

CyberWar: National Security Concern

The United States, Russia and China are in a three-way race for long-term global domination. As told by the Brookings Institute in 2020, a common belief is that the country that leads in Artificial Intelligence (and therefore Cyber and Quantum Computing) by 2030 will global domination for the next 70 years. Russia is furthest behind, with US leading and China stealing US intellectual property to draw within a virtual tie.

> **"Whoever leads in artificial intelligence in 2030 will rule the world until 2100"**
> **- Brookings Institute**

Russia seeks to disrupt the United States in its pursuit. It has overtly claimed an alliance with China. Russia and China both have their sights on the rare earth minerals in Afghanistan and Africa, and they both have made claims on autonomous countries near their borders that the U.S. seeks to defend - Ukraine and Taiwan.

The US economic and national security supply chain critical infrastructure sectors.

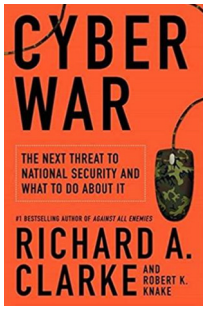
None of the three countries believe direct kinetic military action on their superpower adversaries result in anything less than total destruction. Russia takes military action against the U.S. on our soils, and we will respond united as a country, with the full force of our arsenal. Instead, Russia wants to engage us in an economic disruption to slow our ability to outpace them in this AI/Cyber/Quantum race. They attack the Ukraine by direct military action as well as propaganda, disinformation and cyber attacks of Ukrainian government, medical, military and nuclear power.

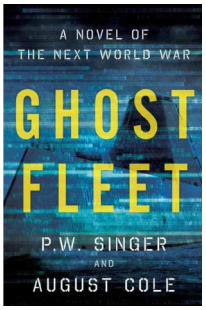
Russia has long managed disinformation campaigns aimed at manipulating the American public to divide the country and weaken our response. Since the United States has little appetite to get involved in another troop deployment after a long Afghanistan entrenchment, non-military actions likely will not provoke a national unity or will to engage in a military war. Therefore, the US responds by not providing military forces, but providing weapons, sanctions and cyber defense and offensive forces. These sanctions and cyber warfare provide Russia the justification it seeks to start attacking US critical infrastructure.

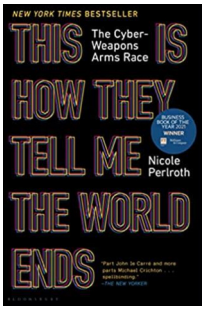
While the battle may result in small military skirmishes in the open seas, space, and other less provocative locations, we should prepare for the United States' economy and national security supply chain to be impacted through cyberattacks. Our critical infrastructure is exposed to cyberattacks, as 2021's disruptions of the Colonial Pipeline and many other victims' operations evidenced. If the US responds poorly, America will have its economy and research advantages eroded to the point that China and/or Russia has global dominance for the foreseeable future. How does the US respond well? America cripples Russia's economy. The US rapidly secures the critical infrastructure sectors and invests in countering disinformation and propaganda. Further, America focuses on calming the political rhetoric and strengthening its military's ability to respond to these provocations. This paper focuses on securing critical infrastructure.

Understanding the CyberWar

While we all understand the impact of a Nuclear War, we minimize the disruption a Cyber War can have. Richard A. Clarke's ***Cyber War***, Nicole Perlroth's ***This is How They Tell Me the World Ends***, and PW Singer and August Cole's ***Ghost Fleet*** spell out the disastrous consequences that arise when our adversaries infiltrate not only our government and military systems, but our critical infrastructure as well. All 16 critical infrastructure sectors operate on legacy systems connected to the internet. The United States has become entirely dependent on the automation and interconnectivity of these systems, whether its our banking infrastructure, our communications, or our operational technologies that create power or drive our manufacturing.







After 9/11, the United States discovered the interoperability of the nation's IT infrastructure was woefully limited, creating issues in our response. The government responded with over $1 Trillion in IT modernization of federal agencies to remediate the interoperability problems exposed by the terrorists attacks. The result is that nearly all IT government contractors saw enormous increases in revenue, profits and values.

The investment in IT modernization and cybersecurity improved the Federal Agencies' ability to respond to cyber attacks. What that did was make Critical Infrastructure the next target. The same interoperability challenge exists today with the CyberWar, just within Critical Infrastructure. Energy, in particular, has a number of challenges making the sector an easy target for Russians. Legacy Systems, lack of ICS/OT skilled cyber workforce, lack of visibility into physical, OT, IT and signal security, and a general lack of vendors and emerging commercial cyber technologies results in highly valued targets being ill-prepared for the CyberWar – and investment opportunities that will yield disproportionate returns.

Brief History of Cybersecurity in the United States

The history of cybersecurity is relatively brief, but its future is long ahead. While the terminology was becoming mainstream only after the turn of the century, the art of attacking and defending attempts at stealing computerized data or accessing and manipulating systems has been on the minds of nations, universities, and engineers since the advent of the computer. The acceleration of computers into every part of our existence has laid the pathways into the data and resources both for ourselves and our adversaries. As the crown jewels of the nation, industry and the individual became easier to reach, the need to build the proverbial wall became impossible to ignore.

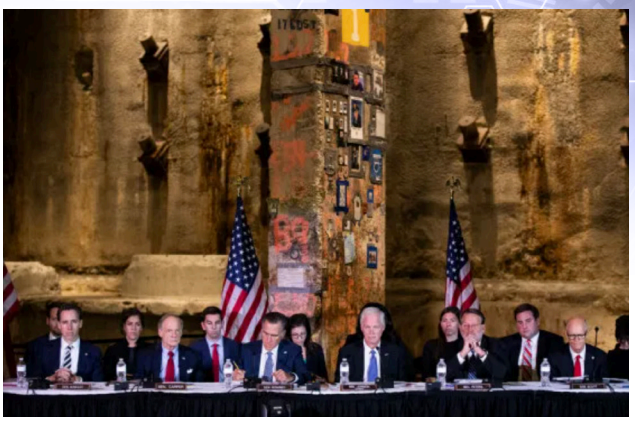
In the 1950s-1980s, the business world enjoyed the competitive advantages and efficiencies brought by adopting the computer into everything from banking to manufacturing. The ability to access records instantly, drive down the error rates of human calculations, drive down labor costs and improve nearly every key statistic incentivized executives to make enormous capital investments. Energy plants built large industrial control systems that would be the underpinning of operations for decades to come. Automobile manufacturers invested billions in computerizing design, research & development, testing, production, supply chain management, scheduling & logistics, accounting & sales databases. The dependency on these systems is the backbone of the improved operational efficiencies, but simultaneously that dependency allows for swift exploitation.

On September 11, 2001, the US saw the worst attack on American soil since Pearl Harbor. The country's response was fraught with operational pandemonium and the lack of interoperability of critical infrastructure was exposed as a weakness and a threat to national security. The Defense Industrial Base and Civilian Contracting market went through a massive expansion after 9/11. The government began investing heavily in C5ISR capabilities (Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance). Interoperability, identification management, automation, autonomy, cyber infrastructure, signal intelligence, threat and anomalous behavior detection, artificial intelligence, cloud and other technology advancements were priorities.

The money for national security focused R&D came from the government, while Silicon Valley was squarely focused on the dot-com world. There were few venture funds in the DC region. In those days, one would take a cautious approach when a government contractor said it wanted to expand into commercial markets.

As a result, starting in the mid-2000s, the United States' cybersecurity activities predominantly focused on national security. The activities rolled out originally from the NSA and other members of the intelligence community to the Department of Defense and the Department of Homeland Security and then to protecting the civilian agencies. That is where the predominance of the attention of the US government landed up until US Cyber Command was spun out from the NSA in October 2010.

Today, America is more exposed than ever before to large scale cyberattacks that could further threaten our way of life. The nation's adversaries are waging coordinated attacks on our government,



Former Homeland Security secretaries testify before Senate Homeland and Governmental Affairs Committee at Ground Zero

defense and intelligence abilities and our business interests. The myriad of challenges weakening our cybersecurity posture is a direct result from having a defragmented system that lacks the authoritarian controls enjoyed by other nations. The result is that our national preparedness to cyber war is weaker than our enemies like Iran, North Korea, China and Russia.

Whereas these monolithic adversaries can mandate the use of national cybersecurity assets, the US simply cannot.

> **Despite the US Federal Government and US Industry being the world's largest investors in cybersecurity innovation, the United States falls far behind our adversaries in getting these solutions disseminated and implemented to protect our national interests.**

This is largely due to the independence of the private sector from the Federal government. While the government mandates regulatory compliance with cybersecurity legislation and best practices, the country lacks control over industries. During an attack on US health care systems, supply chains, financial institutions, telecommunications or electric power and other utilities, the government has little influence to manage a coordinated response. The Intelligence Community may be aware of the threat actors, the FBI may have notified the private company and industry as a whole on the developing cyber-attack, but the response is largely relegated to the hands of corporate executives who have to balance the cost of cyber resiliency with the demands of operating a business.

National Rollout of Cybersecurity Regulations

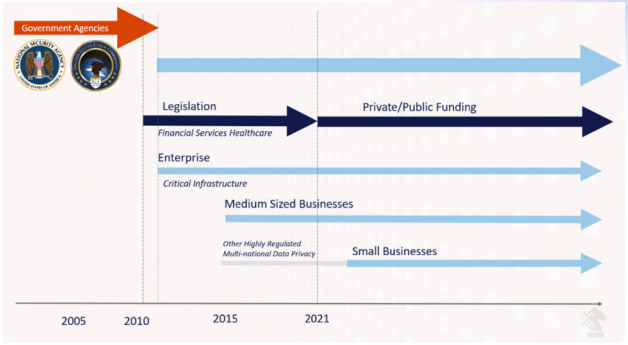
When tracking how the rollout of cybersecurity in the United States occurred, the pattern was to roll out in the US defense, intelligence and homeland security agencies, followed by civilian agencies, then highly regulated enterprises, then to the mid-sized companies. We are just starting to see the small businesses and organizations that are in highly regulated markets being forced to comply with the same regulatory burdens as the enterprise company. Without that mandate, the competitive nature of business means that if a company is not required to invest in a preventative measures they will reserve their resources for other more pressing concerns.

To secure the United States, the government began requiring cybersecurity compliance to federal civilian agencies and has been gradually rolling out more regulatory requirements to each of the highly regulated industries. Since 2010, the government has moved to compliance in each of the highly regulated industries - any industry that has a large regulatory body that is forcing compliance with sets of rules and regulations is subject particularly to new cybersecurity compliance.

Each highly regulated industry faces increasing cybersecurity compliance requirements from their regulatory body and the laws of the States and the US Federal Government.

The Department of Homeland Security deemed 16 sectors as Critical Infrastructure Sectors, making cybersecurity of these mission critical sectors an accelerated priority. These 16 include Chemical,

The US economic and national security supply chain critical infrastructure sectors.



Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste Transportation Systems, and Water and Wastewater Systems.

There are three major categories that the many industries fall within: Federal facilities and systems, Information Technology ("IT") systems and Operational Technology ("OT") facilities and systems. Lastly, there are three major size categories -

01 Enterprises with enough internal resources to effectively manage the cybersecurity challenge on their own.

02 Mid-Sized businesses that have a fraction of the resources but have the same compliance requirements and security issues as their larger peers.

03 Small businesses that are just trying to do enough to not be embarrassed.

Securing the Energy Sector

Russian attacks have thus far targeted Ukraine's critical infrastructure sectors include government, medical, financial services and the energy sectors. As nation-state adversaries cyber-attack critical infrastructure within the US, new advanced cyber defenses need to be mounted. This requires a strategic partnership between the Federal Government, State and Local Regulators and Private Industry.

As the United States' national security is interwoven with private industry and regional utilities, securing critical infrastructure from nation-state and criminal cyberattacks is within the domain of public sector national security. Key to securing these complex systems is a collaboration between federal agencies and the private sector, to ensure that the advanced cyber capabilities and technologies within the US defense and intelligence community get into the hands of the industrial cyber defenders and the private sector, **to ensure that the advanced cyber capabilities and technologies within the US defense and intelligence community get into the hands of the industrial cyber defenders.**

THE WHITE HOUSE

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences

Department of Homeland Security's Cybersecurity & Infrastructure Security Agency calls for sector-specific security partnerships between the public and private sectors that foster integrated, collaborative engagement and interaction. The Department of Energy is the sector-specific agency for the Energy Industry. This was reinforced in President Biden's Cybersecurity Executive Order.

> **The problem is that this Energy Sector Private-Public Partnership is not mature and the crisis is at hand.**

US Federal Government

In this partnership, each party bears responsibilities to manage what the other cannot. The US Federal Government has to bear costs which are too great for private industry, especially those under-resourced entities within the sixteen critical infrastructure sectors.

The Federal Government already supports four major activities that can quickly accelerate the adoption of new cyber defenses:
Research & Development of advanced cyber defenses; Test & Evaluation of organizations' vulnerabilities, exploitabilities, and cyber defensive capabilities; Cyber Workforce Development to train and qualify the industrial defensive workforce; and Subsidies, Grants and Loans to fund the rapid deployment of new OT and IT hardware, software solutions and people. However, the bureaucracy and complexities make navigating the various federal agencies and programs challenging for industry to understand how to access the resources available to the Industrial Cyber Defender.

Cybersecurity Vendors

As noted above, this field of "cybersecurity" is a nascent industry, having started in the intelligence community contractors that supported the NSA and US Cyber Command in 2004. In 2010, the largest enterprises started building their security teams. In 2015, the medium sized businesses found that they didn't have the resources to build an internal team, and needed vendors they could outsource their IT management and cybersecurity to. The cybersecurity consultancies, managed services providers, systems integrators, managed security solutions providers and value added resellers rushed into the market, looking to fill market gaps.

However, the vendors have largely ignored the Energy Sector as the technical characteristics of Industrial Controls Systems, the Operational Technology/SCADA networks present challenges most cyber professionals haven't been exposed to.

CyberWar Technologies Accelerator

Cyber Capital Partners, LLC is a US Department of Defense Trusted Capital Provider and commercializes cybersecurity technologies for the Defense and Intelligence Communities, and the 16 critical infrastructure sectors through its CyberWar Technologies Accelerator.

The CyberWar Technologies Accelerator focuses on emerging cybersecurity technologies and provides the market intelligence, technology planning, customer sprints, investor sprints, new venture creation and operational maturity to ensure these technologies get commercialized and into the cyber defenders' hands. The process was cultivated over 20 years working with advanced R&D technology organizations, government contractors, commercial consultancies, infrastructure providers and security operation centers, the investors, and the rest of the cybersecurity ecosystem stakeholders.

SEARCH

The CyberWar Technology Accelerator's search criteria is built around a set of integrated solutions, modeled after the requirements of the aforementioned Cybersecurity Executive Order, NIST and other cyber frameworks. This solution set is a combination of services and technologies, and aligns with the deal flow we source, vet and syndicate investment capital, customers and strategic partners for.

TEAMING

Cyber Capital Partners' unique access to national laboratories, incubators, accelerators and emerging technologies provides us with a wide range of cyber technologies. We collaborate with additional R&D teams with domain expertise in cloud, quantum, AI, and other advanced technologies, and with service organizations that have customer access to help define the customer requirements.

DEVELOPMENT

The CyberWar Technologies Accelerator addresses the "Valley of Death" that exists for proof-of-concept cybersecurity technologies. These technologies are created by brilliant cyber technologists, who often lack the business acumen, experience, and network to commercialize their inventions. As a result, these start-ups frequently fail to reach the sales targets required to get subsequent rounds of venture capital. Our managed approach ensures the best technologies get through market validation.

> ***To learn more about the technologies and services we prioritize, schedule a call. We welcome the opportunity to assess how your organization and CyberCP can collaborate. We welcome feedback and look forward to meeting with you to discuss this further.***

Jason M Gayl | Managing Partner & CEO | Cyber Capital Partners, LLC