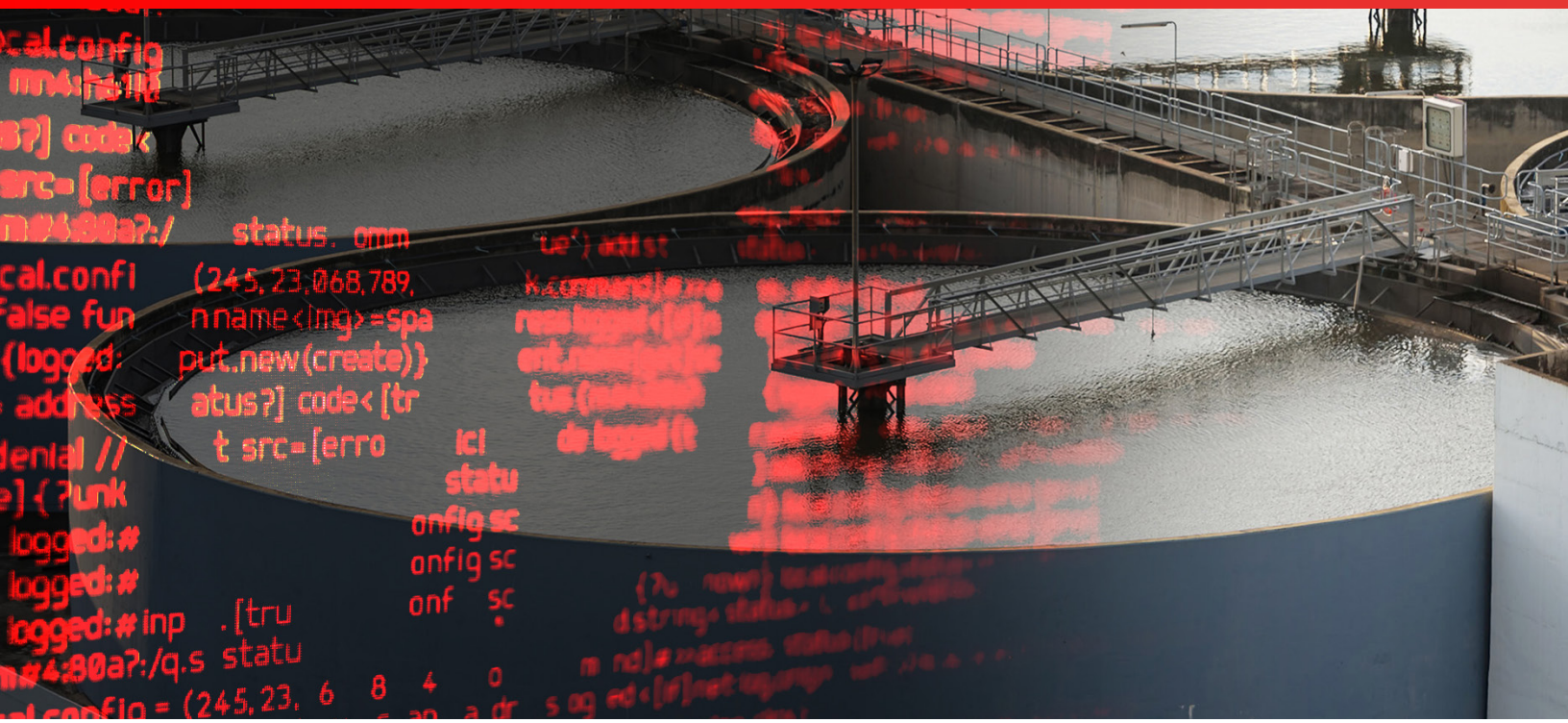


The Impending Cyber Disaster

The world as we know it will end within the decade...
and quite possibly in the next 2 to 3 years.

I am perfectly aware that this statement may sound crazy to normal well-adjusted people, especially in this age of misinformation, conspiracy theories, QAnon paranoia, and other radical notions.

However, as I intend to show, this isn't far fetched, and a lot of experts agree.

This statement is born out of the rapid rise of cyber threats and the utter inability of cybersecurity to see or defend against them.

My name is Ken Tola, and I'm a multiple-patented deep technologist and the cybersecurity expert who founded *Bear Systems*. I've worked on a range of highly sensitive projects including our Visa and Passport system, and the Health and Human Services Emergency Command Center.

- The World Economic Forum (WEC) predicted Covid 4 years before it occurred
- The WEC now predicts a Cyber Pandemic in the next 2-3 years
- It is estimated that 90% of our population will die if this attack is left unchecked

I've seen first-hand how utterly ineffective cybersecurity is against these cyber threats.

And I have realized that hackers are not just attacking for money - rather they are planning a far more nefarious and disastrous outcome.

This document highlights the impending inevitable end of modern society by explaining just how fragile the modern world we live in has become, and why this world as we know it, is doomed to cease to exist.

And it's all because of the deficits of cybersecurity.

BEAR Systems

Executive Summary

We are currently at war. It is a cyber-war, but make no mistake – it is war.

Hostile actors are combating us with increasing velocity, impact, and sophistication.

Rogue hacker collectives operate without any national boundaries or repercussions.

So, the real question isn't when, or where, will the next cyber-attack occur, or how disruptive will it be. The real question is: When will an attack render so much damage that our society is no longer able to function?

The World Economic Forum indicates that over 90% of cyber experts have expectations of this major catastrophic cyber event within 2 to 3 years causing significant impacts to infrastructure and societies, and an end to the United States as we know it.

Cyber threats not so long ago were little more than an inconvenience that resulted in annoyances, rather than anything impactful. Those threats have massively evolved into real-world threats that can destroy equipment and poison millions of people.

Targets include our power plants, water treatment plants, and all of our pipelines, as they are all dangerously exposed. Active targets include critical systems modern society relies upon including banking, food distribution, emergency services, and national defense.

And it isn't simply that our infrastructure lies exposed to a potential attack. Highly destructive malware already infects much of our critical national infrastructure and it is lying in wait for instructions.

And there isn't a damn thing today's cybersecurity solutions can do to prevent it.

Our current best hope is that it creates a mutually assured destruction scenario with both sides showing restraint. But mutually assured destruction only works when both actors are known, and as will be shown, most cyber attackers remain comfortably anonymous.

How Will It Happen?

The attack will almost certainly start with a massive DDoS attack leveraging the *billions of compromised IoT devices* throughout the country and around the globe. The attack will take out all communications and any chance of a coordinated response.

Simultaneously, all the malware hidden throughout our Critical National Infrastructure (CNI) will activate and disable safety control systems, contaminate and *poison water supplies*, erase all facilities data with no hope of repair, damage our power generation facilities, and completely shut down the electric grid.

When the electricity goes out, so does society. Immediately, *all traffic control systems go offline,* gas pumps stop working, home heating or cooling systems fail, potable water supplies are exhausted, medical systems and critical supply chains completely collapse, the financial system freezes up, and people panic.

Generators will buy some places weeks of extra time, but the most critical generators will divert and exhaust remaining fuel supplies, and *within two weeks* of completely losing power, society completely collapses and up to *90% of the US population would die*.

This is not some fantasy, post-apocalyptic TV show, or an alarmist spouting yet another fluky theory. This is going to happen and there is nothing current cybersecurity providers can do about it. Worse, the providers know *they will fail as they always have*.

The truth is that no modern cybersecurity tool can see current cyber attacks – and have been unable to do so since at least 2019.

The reality is that no malware has ever been eradicated. They are all present everywhere and, at best, they are deactivated for the time being.

Time is running out to do anything and the focus has to be on our CNI given the sheer effort involved, the unified political willpower required, and the clock that the WEF started over two years ago.

Our Most Pressing Concern

Modern life is full of struggles including financial concerns, the daily news cycle of violence, geopolitical disasters, the latest global weather disaster, raising children under constant threats of school shootings...

Meanwhile we are rapidly racing toward disaster – extreme weather, violent extremism, threats of a regional war expanding to worldwide conflict, a swelling global population – but the absolutely most pressing issue is cybersecurity.

Wait, "Cybersecurity"?

If you do not believe the depth of the issue, then read this article referencing the *January 2023 World Economic Forum's (WEF) warning* that "over 93% of cybersecurity experts believe 'a far-reaching, catastrophic cyber event is likely in the next two years' ... threatening societies and key infrastructure."

Our Critical National Infrastructure (CNI) is *exposed to extreme danger* from cyber-threats.

CNI refers to the assets and systems essential to the functioning of a country's society, economy, and government. These are typically assets that if disrupted or destroyed, would have a significant impact on the country's security, economy, or public health and safety.

Examples of CNI Include:

- Power generation, transmission, and distribution including oil and gas pipelines and refineries
- Water supply, treatment and distribution systems
- Financial Systems including banking and transaction systems
- Internet infrastructure and telecommunications networks
- Transportation systems, including railways, and airports
- Healthcare facilities and emergency services
- National security, law enforcement and emergency management
- Food supply chain systems, including distribution

Serious cybersecurity warnings from global experts have resulted in nothing short of a complete lack of true action to date. We've got to get our heads out of the sand.

The WEF has gone as far as to *directly compare this cyber pandemic to Covid*. Whether you think they are really smart or the culprits, the inevitably of this global attack is very real

This paper aims to explain why such dire warnings are correct and why cybersecurity is today's most pressing fundamental threat to the foundation of modern society.

Setting The Scene

Oil Rigs – Deepwater Horizon

On April 20th, 2010, the Deepwater Horizon Oil Rig exploded in the Gulf of Mexico killing 11 people, releasing 210 million gallons of oil, and causing over $17B in damage. The official explanation attributes the disaster to a combination of factors, including a failure in the blowout preventer and "poor management decisions".

At that time, I was in contact with numerous people in charge of protecting our ports and Critical National Infrastructure. These people explained to me that forensic evidence indicated a Chinese hacker infiltrated that blowout preventer on the oil rig and turned it off, but was unable to turn it back on.

Given the geopolitical risk, this group surmised the hack was an exploratory effort and not a deliberate attempt to destroy the rig. As I'll demonstrate later, this follows a common cyber tactic – to detect vulnerabilities, gain access and gather more information, and then use that information to expand the reach of a threat to inflict maximum damage, if or when deployed.

The group's findings were presented to Big Oil executives along with a remediation plan to replace every pressure sensor on every oil rig – and it would cost billions, which was deemed too expensive. That particular threat, and others like it, continue to exist on oil platforms, with a tacit understanding that a coordinated attack on the oil rigs would result in a mutually assured destruction scenario.

But decentralized rogue hacker consortiums don't follow orders from governments, which leaves the threat looming.

The official stance on the Deepwater Horizon disaster hasn't changed, however the Government Accountability Office (GAO) is finally starting to *bring awareness to the issue*.

Operational Technology (OT) includes sensors and command and control systems that are reliant on digital communications.

Where communications paths exist, the threat of a cyber attack is ever-present.

Public Utilities

Similarly, I worked for a group that built utility energy demand/response systems. During this time, I toured different power plants to understand their control centers and met the main IT officers. I asked them about their cybersecurity situation and response plan.

They immediately admitted they were exposed and at risk to cyber-attacks, a systemic problem confirmed *by Moody's* last year.

When asked about their response protocols to a cyber attack, the person in charge pointed to an identical backup system and explained they would roll over to the backup. When I pressed further, asking why the same attack couldn't be replicated on the identical system, his response was one that I've found to be typical – putting one's head in the sand – he shrugged his shoulders and walked away.

As if that wasn't enough – I later met an ethical hacker who told me about his flight from LA to New York. He booted up his laptop, connected to the airplane's Wi-Fi and searched for others connected to the same in-flight Wi-Fi.

He found another traveler on the Wi-Fi, gained access to their poorly secured laptop and discovered that this traveler had left open a remote terminal session to their home computer where management software for a major utility was running. He quickly determined that he could turn off the entire utility, and figured it would have taken down about 20% of the country's electrical grid – if *not the whole thing*.

He accomplished all of this between boarding the plane and before people could move freely about the cabin after takeoff. He showed me time-stamped screenshots of the entire process to prove it.

Thinking maybe this could all be made up?

Read this article about *the three known water treatment plants taken down in 2021*, and this one about the electrical plants that were *hacked last year* or how *Denmark was compromised*.

Nuclear Power Plants

As I've indicated, I've worked on a lot of different systems and projects, and while working to evaluate nuclear power for a Smart City project, I was introduced to one of the larger nuclear power plant manufacturers in the world to assess their vulnerability to cyber attacks and hacking.

Their response to my questions indicated that they secured nuclear power plants by isolating the different sections of the plant using multiple non-interconnected physical networks. They explained that completely separate and disconnected "air-gapped" networks immunized the entire reactor against compromise.

When further questions revealed they allow remote plant management, I asked how that was possible given the isolated networks. Their incredulous response was that they enable remote access through a Virtual Private Network (VPN) so that someone with the proper credentials could access anywhere within the plant at any time.

I bluntly pointed out the obvious – that remote access effectively tore down the air-gapped security between their networks and exposed the entire plant. And that's when they ended the call.

> Remember the story about the ethical hacker on the flight?

That experience makes *this article from Charles Hamilton* one of my favorites. Charles Hamilton is an expert at penetration testing – the process of ethically hacking into a system to discover and patch vulnerabilities. He has hacked numerous power plants including nuclear power plants.

More disturbing articles? *Other* nuclear power plant *attacks* that occur nearly *every day*. The threat is clear and present.

Is Anybody Home?

The looming *cyber pandemic* will start with an innocuous knock on our cyber door...

Probing Defenses

With either a physical or cyber attack, the strategy in attacking a larger target is to first probe the defenses. Equally important is remaining undetectable and untraceable. To attack something as large as a country, the target must be well-defined.

Are Defenses Being Probed?

This is the nature of the Pentagon's concern about the discovery of numerous unidentified objects penetrating N. American airspace starting with the Chinese spy "weather" balloon in February, 2023.

Probing defenses is an iterative testing process resulting in modifications to tactics and strategies that lead to increasingly larger, or more penetrating attacks.

The goal is to understand the speed, type, and depth of responses, and how the discovery of any given attack was made. Those learnings expand knowledge of the target, leading to even larger-scale tests.

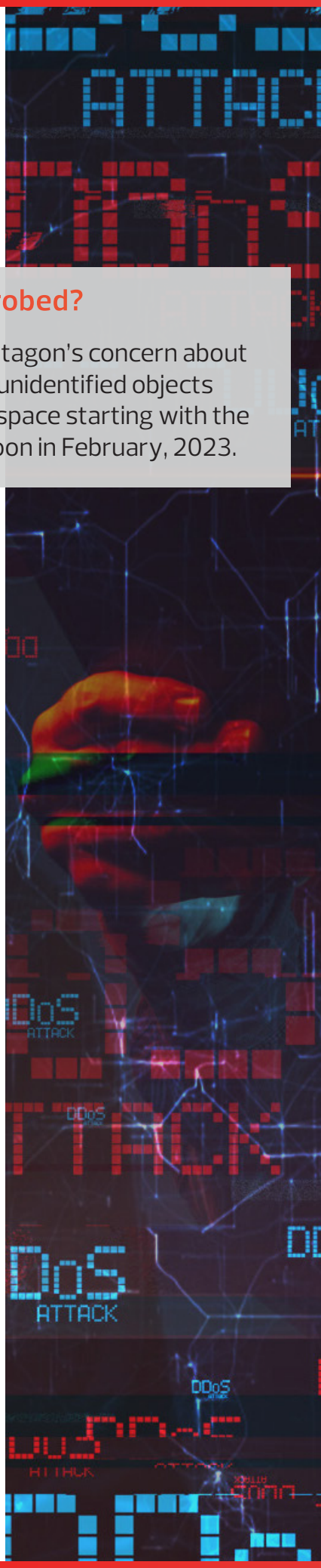
To this end, hackers leverage Distributed Denial of Service (DDoS) attacks. A DDoS attack results in overwhelming the targeted website, network, device etc., to the point where the system is unable to function, effectively taking down services and operations. For government and financial institutions, these *operational outages can cost millions of dollars* per hour.

DDoS attacks *readily reveal the intricacies* of any given target and have been used for years as a cover for injecting additional threats into overwhelmed target systems.

Increasingly Sophisticated Probes

The evolution of the DDoS attack started in 2007, launched on behalf of Russia for political reasons against *the country of Estonia over the course of 22 days*. While this initial attack lacked sophistication and did little actual damage, it was attention grabbing and multinational hacker collectives started using the techniques and evolving the strategies.

In 2013 a DDoS attack resulted in *taking an entire company offline* for the first time. It occurred against the largest anti-spam provider in the world, Spamhaus. When their hosting provider, Cloudflare, attempted to intercede, the hackers went after Cloudflare's infrastructure. Brian Krebs, one of the foremost experts in cyberwarfare, provides a fascinating *insider view of this attack*.



The next major attack came in 2015 and was again aimed at a single company – this time *GitHub was taken offline*.

What made this attack unique was the increasing sophistication. The hackers *leveraged China's Internet infrastructure* to launch the attack. China received international blame and predictably both denied the attack and covered up their exposure. But the truth remains that a large hacker collective took over one country's infrastructure and used it to attack an asset in another country while effectively misdirecting the blame and response back onto China – all while remaining anonymous.

Leveraging Anonymous Sources

As previously mentioned, a main goal for any adversary going after a larger target is to remain hidden. This capability first became a reality with the advent of the Mirai Botnet.

Mirai was the first attack that was able to *take over control of Internet of Things (IoT)* devices such as printers, security cameras, and other smart devices. Hackers then used the IoT devices to maliciously flood data to servers and cause major Internet outages across a large geographic area, the eastern United States, while taking down popular sites including Twitter, Netflix, Spotify, AirBnB etc.

Botnets

A botnet is a network of computers, smartphones, or other Internet-connected devices that have been infected with malicious software and are controlled by the attackers.

Botnets can be very large and powerful, and difficult to detect and dismantle, often consisting of tens or hundreds of thousands of infected devices.

Further evolutions of the Mirai botnet attacked financial institutions in the Eastern US. Those attacks started to scratch at the underpinnings of the financial systems in a global finance capital, New York City.

Researchers and investigators are still completely unable to track down the controlling servers or determine who or from where the attacks derived.

In June of 2022, a DDoS botnet attack using over 170,000 different

devices spread over 180 countries, flooded an unnamed Chinese telecommunications company with over 25.3 billion requests. It took hours for *Imperva to stop this attack*, and again, the true source of attack remains unknown.

Mirai hasn't gone away – it is still present on millions of IoT devices and Mirai derived DDoS attacks have continued to grow in size and scope, with attacks progressing for extended periods of time before being halted. Marai, while first launched in 2016, is still actively used today and was just responsible for the l*argest DDoS attack to date*.

Ubiquitous Probes

The pattern of shutting down Internet traffic using distributed attacking resources and misdirection continues to grow. Attacks are increasingly *more complex, powerful and sophisticated*, on ever larger targets, with constantly evolving tactics and strategies – all while successfully shielding the attacker.

Despite this growth, the public has remains unconcerned with the threat, as probes occur with impunity and nobody seems to care. However, the objective of these and many other types of attacks is to learn and become more resilient to defensive strategies.

These attackers now possess the ability to completely shutdown the Internet, but that is not the end of the world...right? I mean, the world ran without the Internet before, and while not being able to connect on SnapChat would suck, it's not the end of the world to anyone but a teenager... Right?

Life Without Connectivity

To be clear, everything in our modern society depends on computers and the Internet – banking, phone communications, global GPS systems, manufacturing, shipping, food production and distribution – everything.

People getting lost without GPS is not a real societal problem, but phone systems would fail, planes would not fly, shipping would come to a standstill, and our *supply chain* would quickly breakdown as everything from manufacturing to delivery relies on connectivity.

In 2015, a major Internet optic cable was cut by vandals causing a shutdown that literally *stopped everything in its tracks*.

With banks immediately offline there would be no way to withdrawal or transact money. The same is true of our medical systems, traffic systems, and emergency services.

Yet electricity would still work, gas and heat would still be viable, and

humans tend to come together in adversity. A total communications breakdown is not enough to unravel society.

The Inadvertent Weapon

These testing probes were never intended as a primary weapon.

As discussed, DDoS was an attempt to simply probe and test defenses to learn more about target systems in order to enable far more damaging attacks on their targets.

The rise in their sophistication and their success in taking down communications is an unintended boon, as completely shutting down of the Internet takes everything down – including any coordinated responses from our government or military.

This simple probing tool has grown into a powerful weapon – and that is all in thanks to the completely inept world of cybersecurity.

Defining The Target

While targeting large companies provided the testing grounds, the real focus is the US government. Taking down our CNI will take down the government and military, and society will follow.

The first documented cyberattack on Critical National Infrastructure (CNI) *occurred in 2001 in Queensland, Australia* when a sole hacker released 265,000 gallons of raw sewage from a waste management system.

The attack exposed serious flaws in the Supervisory Control and Data Acquisition (SCADA) software that runs CNI equipment everywhere in the world. While cybersecurity has futilely attempted to correct these issues, SCADA remains *wide open to attack*.

> SCADA was built for fast, efficient, communications – prior to the advent of the Internet, a time in which the inherent isolation of SCADA systems meant protective measures were scarcely considered.

SCADA attacks evolved from simply siphoning systems data in order to learn how a facility operates – starting with *Night Dragon* in 2006, and even more sophisticated information stealing malware such as *Duqu, Flame and Gauss* – to actual CNI facilities disruption and physical destruction.

In 2008, SCADA attacks resulted in the *Turkey pipeline explosion* right before the Georgia war with Russia.

In 2010 the US exploited issues with SCADA, infecting 14 industrial sites in Iran to take out Iran's uranium production using a computer worm named *Stuxnet*.

And in December 2017, *Triton was discovered* in a Saudi petrochemical plant. Triton was designed to attack and kill humans working at a facility by targeting the SCADA safety control systems that could release toxic gases or cause explosions.

The Triton malware appears to have been inside the Saudi facility's network since 2014, slowly penetrating and exfiltrating facilities data to understand its operations while worming into the most lethal systems.

The perpetrators of those attacks have never been identified and the malware command and control servers have proved impossible to track. Furthermore, the malware has spread to other targets outside the Middle East including North America.

In 2018, *BlackEnergy3* was released, which took down the power grid in the Ukraine – a power grid that is essentially the same as the one operating in the US and EU.

BlackEnergy was originally designed for DDoS attacks. The current version uses the DDoS strategy as a Trojan malware distribution mechanism focused entirely on SCADA.

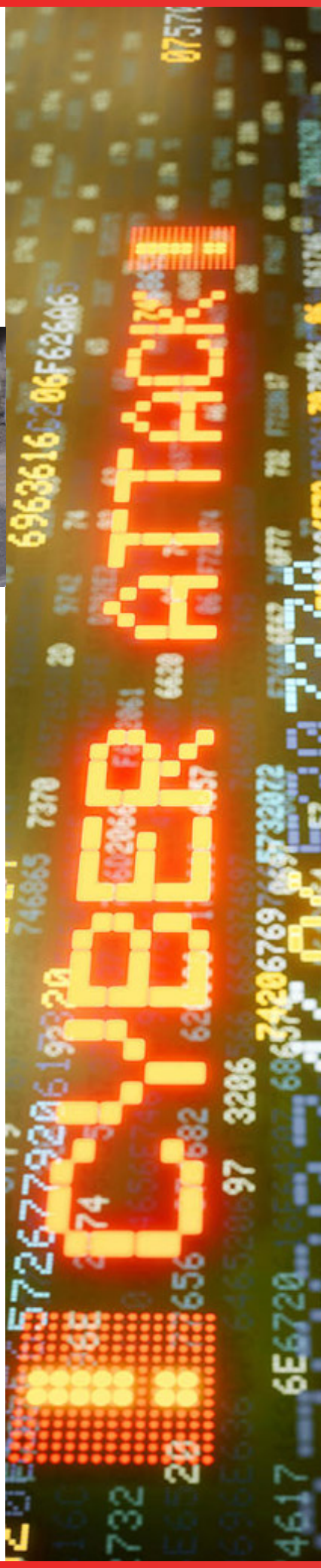
While BlackEnergy could take out the entire power grid of the United States, most CNI possesses the ability to rollover to some level of backup – as long as the core systems data is intact.

Enter *Shamoon,* which goes after facility data and backups and erases everything. The data is not sent out or encrypted to demand ransom – it is simply erased. The Iranians attacked the Sands Corporation with Shamoon in 2014 in retaliation for public anti-Iranian comments by then CEO, Sheldon Adelson.

Now we see the comprehensive and lethal SCADA destruction playbook. Flood communications, infiltrate systems, damage facilities, erase and destroy backup software and data, and *trigger lethal attacks on the very operators* that could respond to the attack by switching to backup systems.

Combining Attack Vectors into a Lethal Package

The rise of infrastructure destroying malware has been swift and methodical and all these tools have come together in a very sophisticated and destructive SCADA malware package called *CrashOverride*.



Instead of a specific piece of software, CrashOverride provides a completely automated malware system for attacking SCADA and Industrial Control Systems. Upon triggering the malware, automation takes over allowing it to spread and inflict extensive damage capable of taking out large swaths of a power grid.

The infiltration for such an attack on CNI in the US has already occurred. The Department of Homeland Security (DHS) admitted to the *extensive infiltration of the US power grid* by the Russians.

Russia, of course, denies the allegations, however the strategy has been to position a culpable nation state (be it N. Korea, Iran, China or Russia) to take the blame for a CNI attack, raising the stakes of international conflict.

And as evidenced by the state of emergency declared on the East Coast after the *Colonial Pipeline* attack, there are latent threats throughout US CNI, with continuous attacks probing corporate, government, and private systems. Every day. Every hour. Every second.

The attack pattern on CNI is obvious. Attacks started small and rapidly grew in complexity, while continually probing and testing with increasingly sophisticated and automated tools that are distributed across the world. These systems run from command and control servers that are impossible to locate, by skilled and stealthy strategists who infiltrate systems with self-replicating malware, and carefully plan an assault over many months or years.

They are well-funded and use methodical tactics to steal information and study the networks, reverse engineer the systems, siphon operator credentials, then they prepare a well-synchronized completely automated assault to either test, take over, disrupt, or destroy infrastructure.

And then they learn how to improve – based on detection time, response time, and response tactics – to leverage ever more lethal threats into our CNI.

Meanwhile cybersecurity can do nothing to stop them.

Attacks are moving into extremely dangerous realms with a recent attack in Florida *attempting to poison millions* of people, followed by a *separate attack a few months later* attempting the same result.

Live Threat Report Maps

Kaspersky
https://cybermap.kaspersky.com/

Net Scout DDoS Attack Map
https://horizon.netscout.com/

Fire Eye Threat Map
https://www.fireeye.com/cyber-map/threat-map.html

Spamhaus Map
https://www.spamhaus.com/threat-map/

DDoS is clearly capable of getting malware into systems with seeming impunity. The final piece to this puzzle, however, is where to hide these dangerous agents long term to avoid detection.

Hiding in Hardware

Hackers hide their agents and trojans in low level software, and now, in nearly indiscoverable locations on the underlying hardware.

While viruses and malware have been around even longer than the Internet, hardware was not leveraged until *Rakshasa appeared.* Rakshasa created the first backdoors on attacked hardware, enabling hackers to gain unfettered access to a compromised system.

Current cyber tools *almost always fail to find backdoors*, as backdoors do nothing to attract attention when not in use, and are usually discovered through log files hackers mistakenly leave behind.

A hardware or software backdoor is an open pathway to an impacted device. Software backdoors have become somewhat easier to detect, but only on traditional networks. Hackers still get away with adding or corrupting system files, but counter efforts might eventually render software backdoors obsolete. Hardware backdoors however are another story, and they are extremely difficult to detect in systems such as CNI.

As related previously, Stuxnet targeted Iran's CNI. Importantly, Stuxnet was the first worm to overcome hardware protection by faking security credentials. Using this technique Stuxnet buried itself deep into the hardware underlying the SCADA systems and remained hidden until told to attack.

Given the serious nature of national security and a direct attack on Iran, the details of how Stuxnet was deployed are unconfirmed but fall into two camps.

One theory is that Stuxnet was not deployed straight to Iran, instead it was *released into the wild and wormed it's way into Iran's systems*. Another report based on *"The Perfect Weapon"* posits that it was directly deployed to a facility system through wireless transmission from miles away, and has since wormed it's way out.

Regardless, Stuxnet infected CNI equipment globally, has yet to be eradicated, and is now exploitable by rouge nations and hacker collectives everywhere.

While injecting malware into hardware is one approach, an even more devastating attack was blamed on China a few years ago.

In October of 2018, Bloomberg *broke a major story* on how China embedded a tiny, rice grain-sized chip that did not exist in the original designs of Supermico, a major hardware manufacturer providing equipment utilized by major Cloud providers such as Amazon's AWS and Apple, and also used throughout the Department of Defense.

An on-going, secret investigation into the source of the chips supposedly discovered that the Chinese government compromised four subcontracting factories by threatening or bribing plant managers to alter the original designs.

Even though this type of attack might seem obvious, ***nobody ever detected the issue on the hardware***. It was only the breakdown of the people producing these compromised components that led to their discovery.

Despite figuring out the issue, the U.S. government has done *little to nothing to remedy this issue*.

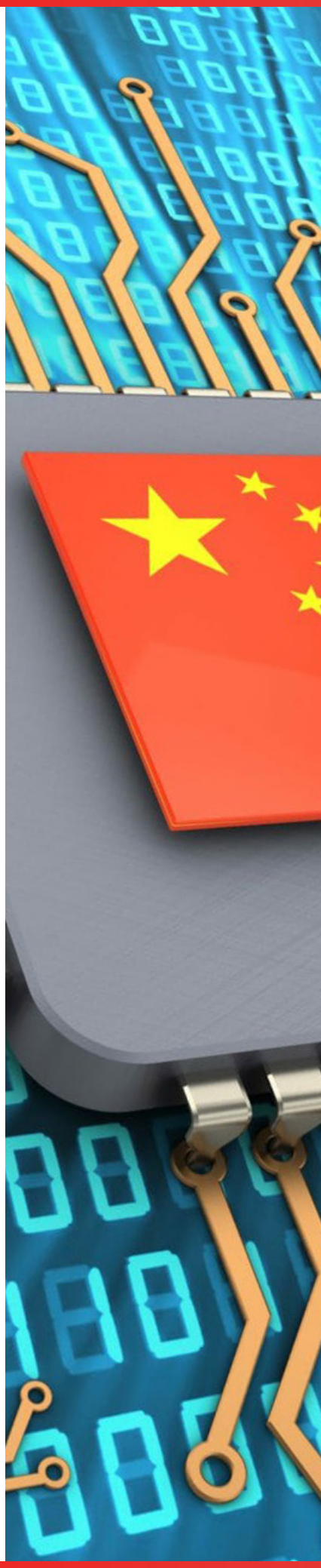
A device's main hardware manager is the BIOS. The BIOS not only controls the hardware, it literally tells the operating system, and cybersecurity applications, what hardware exists on a device. And it is *continuously hacked*. Hacking the BIOS results in the ability to hide any malware with no concern of detection.

This problem was exacerbated in 2019 when all Qualcomm chips were *revealed to have a hardware backdoor* that would allow hackers to store information without detection. A *problem that still exist in Qualcomm chips* throughout the world today.

At this point, we were contacted by several large government groups asking if we could protect their mobile devices and core servers. This was part of a larger effort by the US government to find any solution to a series of well known hardware vulnerabilities.

Hardware, as it turns out, is the perfect place to embed attacking agents for extended periods of time.

And the *attacks to place these agents* are occurring on the US power grid at an exponentially increasing rate.



Hiding In Plain Sight

Sunburst was one of the first examples of a disconcerting evolution in cyber attacks – one that cyber providers strive to hide.

To understand the threat, it is important to understand that modern cyber products use log files to obtain all of their information about what is going on in a given system. Log files are text outputs a given operating system provides at different levels of activity and are supposed to be historical records.

The problem is that no modern cybersecurity product can directly see what is going on within a given device – hence log files.

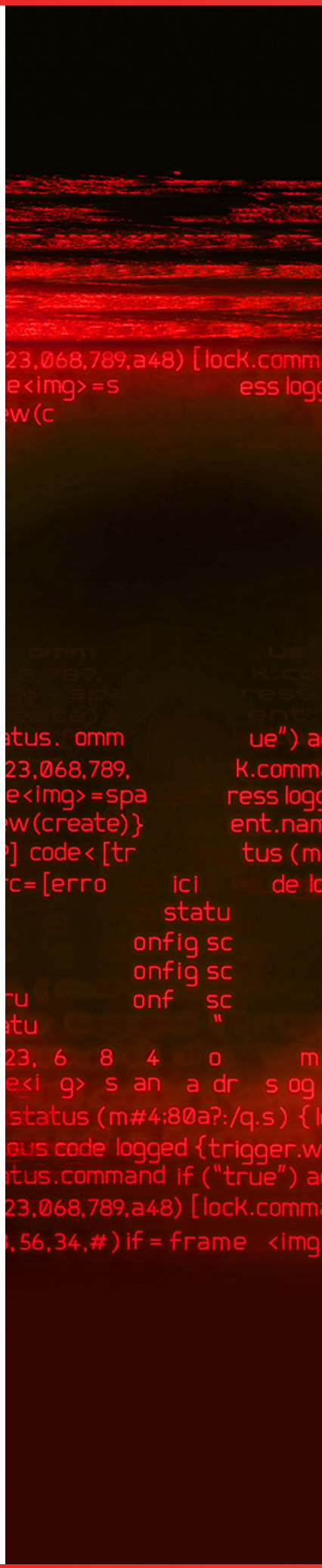
That evolution? Modern attacks have figured out how to *modify log files in real time* as well as how to *prevent any logging* of certain activity such as communications. Thus all modern cyberattacks are *completely invisible* to anything cybersecurity vendors can provide.

In fact the only tool that provides any help are the circa-1990's signature matching anti-virus programs that sometimes see abnormal files or memory objects. While *it is easy to hide from these tools*, they can get lucky on occasion. Modern cybertools refer to these abnormal results as Indicators of Compromise or IoC. If enough IoC are found then a cyber expert is sent in to manually look at the suspect devices.

There are *online courses available on YouTube* that teach malware writers how to turn themselves off when an admin logs into a device. This simple solution renders manual inspection moot and is why it took cyber *experts nine months to find Sunburst* after it was determined to be a threat.

Currently there is no protection against ransomware, which is why the *Colonial Pipeline had to shutdown for a week*. There is nothing to prevent data from being sent wherever a hacker desires, which is the main threat of the *current MoveIt attacks*. There is nothing to stop backdoors from being placed into systems and nothing that can see of stop those backdoors from being used which is the crisis underlying the *Citrix Bleed attack*.

The new wave of cyberattacks have overcome all modern cybersecurity capabilities once they get into a system. Since cybersecurity understands this fact, their collective efforts are focused on preventing intrusion. Unfortunately, this effort is a zero sum game as *2023 set the record for the most data breaches*. Further, this approach does nothing to address *the completely compromised government systems* and *CNI*.



Escalation

As the end draws closer, you would expect to see a further rise in the severity and number of attacks, and in fact, several recent incidents point to a rapid escalation of attacks on hardware both as proofs of concept as well as more insidious wide-scale placement efforts.

The latest types of attacks, which include Sunburst, Citrix Bleed, and MoveIt, all leverage a new exploit that nests compromised files within legitimate software. The frequency of large-scale attacks stemming from this new vector are increasing in frequency to the point of now having overlapping active exploits.

> Cybersecurity as an application results in almost all the issues plaguing cybersecurity today – as applications are simply the wrong place to provide effective protection.
>
> That has to change.

That makes the *Sunburst attack in December 2021* even more disconcerting. This attack enabled complete access to all government and military servers, systems such as Microsoft's and Google's enterprises and it even used a major cybersecurity company's software – SolarWinds – to complete the attack. For some unknown period of time, an unknown series of hackers had unrestricted access to all of these systems. All of them.

Do you really think they would not place malware everywhere?

As for more evidence of the increase in escalation, the recent FAA outage is a perfect place to focus. As is the case with any government outage, the *January 11th outage of the FAA systems* was sold as human error - someone making a simple mistake.

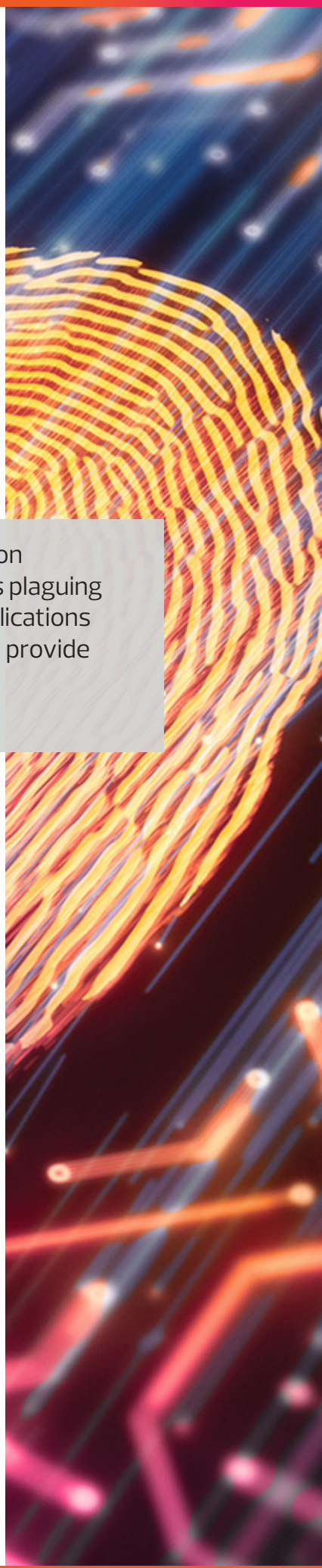
Yet, the *same system was disrupted a few hours later*, only this time in Canada. The systems are not connected and now the *White House is backtracking* on this not being a cyber-attack.

We have three overall stages at play right now.

The first, and most obvious, are continuous assaults across every sector of our institutions – from schools to CNI. This is a staging process, planting and inserting assets positioned for attack.

The next stage will take out communications through massive DDoS attacks, coordinated with the final stage – destruction of US CNI.

At that point, the US will be defeated – without anything actually touching down on US soil – with the end result being the self



destruction of a society by its own hands as people begin to miss meals. Just recall the fighting over rolls of toilet paper during Covid to put some context around how desperate people will behave.

Call To Action

I would love to now show you the solution to all of these problems and, in fact, *Bear possesses the technology to address these issues*. That stated, the challenge extends far beyond technology as it requires the willpower of people to push their leaders into action.

I remember when I tried working on cyber protection for cars that a major manufacturer told me the story of anti-lock brakes. While everybody knew for decades that anti-lock brakes saved lives, it was not until the cost of litigation grew too high that the government finally required anti-lock brakes by law.

If we attempt to use this approach in cybersecurity all we will end up solving in global warming and I do not think the mass casualties will be worth it.

The hard truth is that all systems in the U.S. government are compromised, including all utilities. The harder truth is that the U.S. is far ahead of most other countries in terms of cyber protection. If we do not act now, there will be nothing to save us from this civilization level threat.

Spread the word. Raise Awareness.

Do Not Think You Will Not Be Impacted.

#Cyberpandemic

https://bearsystems.com