## 1

#### Tech can solve infrastructure concerns but needs to be integrated – operators are key.

Jacobs 5/31 [Lionel; Senior Security Architect in the Palo Alto Networks ICS and SCADA solutions team. Coming from the asset-owner side , Lionel has spent more than 20 years working in the IT/OT environment, with a focus on ICS systems design, controls, and implementation. He was a pioneer in bridging the IT-OT security gap and implementing next-generation security into performance and safety critical process control areas. During his tenure, he successfully deployed a large scale ICS/SCADA security architecture composed of over 100 next-generation firewalls, hundreds of advanced endpoint protection clients and SIEM, distributed over dozens of remote plants and a centralized core, all based on a "Zero Trust" philosophy. Lionel graduated from Houston Baptist University with a double degree in Physics and Mathematics and has held certifications as a MCSE, CCA, CCNP, CCIP, CCNA, CSSA, and GICSP; “Critical Infrastructure Protection: Physical and Cyber Security Both Matter,” eSecurity Planet; 5/31/21; https://www.esecurityplanet.com/networks/critical-infrastructure-protection-physical-cybersecurity/]//SJWen

Segmentation based on business criteria

Segmentation is not just breaking apart the network based on the IP-Address space. True segmentation requires identifying and grouping devices into Zones or Enclaves based on meaningful business criteria to protect better vulnerable devices found within the address space. Access to devices in the zone needs to be restricted by users, groups, protocols, networks, and devices. In some instances, you may even consider restricting access by time of day.

IoT/IIoT is beginning to take hold in the energy industry, which means there are going to be more devices attached to these networks gathering information and possibly running on a vendor’s proprietary software and hardware, which more than likely will not be managed or patchable by the operator of the system. So O&G needs to have a definite plan on how they will address this growing trend, and a zero trust-based strategy offers the best means of doing this integration in a safe, secure, and, most important, reversible manner.

Camera and sensor security

Segmentation will also include the zoning of radio frequency (RF) technologies like Wi-Fi, Microwave, satellite, and cellular. ICS and SCADA systems operators must remain mindful of the possibility of an upstream attack by threat actors who have managed to compromise their RF facilities. Remote facilities and devices often have cameras and sensors to alert when a door has been opened. Still, because they are remote, attackers have time to enter the facilities and plant a device that can go completely unnoticed.

Another option physical access affords them is the opportunity to compromise the runtime operating systems and/or OS of the devices they find. The only way you will find these would be to do a physical search of the facility or cabinet and run an audit of the OS to ensure nothing has been tainted.

Zoning limits damage

So the reason why the zone trust segmentation (zoning) is so important is if you don’t have the time to perform these acts to confirm that the site is not compromised. With proper zoning enforcement, you can limit and isolate the damage to a region or just that location.

Zones in a Zero Trust network also serve as an inspection point for traffic entering and exiting the enclave. The enabling of IPS, IDS, and virtual sandboxing technology can be applied on a per-zone basis, allowing for customized protection for the vulnerable devices contained within. Implementing these security measures is a best practice even on zones where devices can receive updates and have some form of endpoint protection.

With proper design and device consideration, zoning with the different inspection technologies enabled can also be a remediating factor for those devices in your network that cannot be patched, updated, and even those that are end-of-life. In short, zoning with inspection technology enabled helps to ensure IT and OT network systems’ safe operations. In even the most secure environments, it is never safe to assume that data traffic transversing the network is free of a potential threat.

#### Increased strikes send a clear signal to terrorists that critical US infrastructure is vulnerable by weakening organizations.

Davies 6 [Ross; George Mason University - Antonin Scalia Law School, Faculty, The Green Bag; “Strike Season: Protecting Labor-Management Conflict in the Age of Terror,” SSRN; 4/12/06; https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=896185]//SJWen

Strikes (and, to a lesser extent, lockouts) are painful but necessary parts of private-sector American labor-management relations. Even if they weren't - even if sound public policy called for their eradication - we couldn't stop them. They are an inevitable byproduct of the conflicting interests and limited resources of organized workers and their employers. History shows that this is true even in times of warfare overseas or crisis at home: labor-management strife lessens at the beginning of a conflict and then bounces back. Now, however, we are confronted with warfare at home, a phenomenon that the United States has not had to deal with since the Civil War - before the rise of today's unprecedentedly large, complex, and interdependent economy and government.

And history is repeating itself again. After a lull at the beginning of the war with terrorists, work stoppages have returned to their pre-war levels. The overall rate of strike activity is substantially lower than it was during previous wars (it has been slowly declining, along with overall union membership in the private sector, for decades). Today's war, however, is being fought in part on American soil, and against enemies who operate worldwide, but whose attacks tend to be small and local, seeking advantage from the unpredictability and brutality of the damage they inflict rather than from its scale. Thus, even small, localized, and occasional work stoppages - not just the large-scale strikes that arguably affected the military-industrial complex and thus the war efforts in the past - have the potential to increase risks to critical infrastructure and public safety during the war on terror. In other words, persistent strike activity at current levels poses risks of public harm, albeit risks that are difficult to anticipate with specificity in the absence of much experience or available data. This justifies taking some reasonable precautions, including the proposal made in this Article.

By its very nature, a labor strike increases the vulnerability of that employer's operations to a terrorist attack. A strike is an act specifically designed to disrupt and weaken an employer's operations, for the (usually) perfectly lawful purpose of pressing for resolution of a dispute with management. A weakened organization or other entity is, of course, less capable of resisting and surviving exogenous shocks, whether they be commercial competition or terrorist attacks. In the United States, with its fully extended and endlessly interconnected critical infrastructure that touches everything from food processing to energy distribution to water quality, a strike in the wrong place at the wrong time that disrupts and weakens some part of that infrastructure could be decisive in the success or failure of a terrorist attack of the small, local sort described above, on such a weakened link in some infrastructural chain. Of course, none of this is to suggest that any union or its members (or any employer or its managers) would knowingly expose their fellow citizens or their property to a terrorist attack. To the contrary, experience to date suggests that union members are at least as patriotic and conscientious as Americans in general. In fact, the effectiveness of the proposal made in this Article is predicated in part on the assumption that neither workers nor their employers will knowingly contribute to the incidence or effectiveness of terrorist attacks. The concern addressed here is, rather, that innocent instigators or perpetuators of a work stoppage might unwittingly facilitate a successful terrorist attack or aggravate its effects.

#### Attacks on critical infrastructure collapses the economy through multiple avenues.

FAS 6 [DCSINT Handbook No. 1.02; Info directly from US army and Deputy Chief of Staff for Intelligence; “Critical Infrastructure Threats and Terrorism,” DCSINT/FAS; 8/10/6; https://fas.org/irp/threat/terrorism/sup2.pdf]//SJWen

Agriculture

In 1984, a cult group poisoned salad bars at several Oregon restaurants with Salmonella bacteria as the first recorded event of bioterrorism in the United States. This resulted in 750 people becoming sick.24 A review of the agriculture infrastructure results in vulnerable areas such as the high concentration of the livestock industry and the centralized nature of the food processing industry. The farm-to table chain contains various points into which an attack could be launched. The threat of attack would seriously damage consumer confidence and undermine export markets. Understanding the goal of the threat points to the area most likely attacked. If the intent was economic disruption the target would be livestock and crops, but if the intent was mass casualties the point of attack would be contamination of finished food products. Damage to livestock could be very swift, the USDA calculated that foot-and mouth disease could spread to 25 states in 5 days.25 CDC is presently tracking and developing scenarios for the arrival of Avian Flu.

Banking

Prior to the destruction of the Twin Towers, physical attacks against the banking industry, such as the destruction of facilities, were rare. Unfortunately, evidence indicates that may change, in March 2005 three British al-Qa’ida operatives were indicted by a U.S. federal court on charges of conducting detailed reconnaissance of financial targets in lower Manhattan, Newark, New Jersey, and Washington, D.C. In addition to video taping the Citigroup Center and the New York Stock Exchange in New York City, the Prudential Financial building in Newark, and the headquarters of the International Monetary Fund and the World Bank in Washington D.C., the men amassed more than 500 photographs of the sites.26 The Banking infrastructures primary weakness is along its cyber axis of attack. Through phishing and banking Trojan targeting specific financial institutions, attackers reduce confidence among consumers. Recently American Express posted an alert online, including a screenshot of a pop-up that appeared when users log in to its secure site.27

The attack not only attempts to obtain personal information that can be used for various operations, but also launches a virus into the user’s computer. CitiBank, and Chase Manhattan Bank have both been victim during 2005 and 2006 to phishing schemes misrepresenting their services to their clients.

Energy

Recently the oil industry occupied the headlines, and the criticality of this infrastructure is not lost on terrorists. In mid-December 2004, Arab television aired an alleged audiotape message by Usama bin Laden in which he called upon his followers to wreak havoc on the U.S. and world economy by disrupting oil supplies from the Persian Gulf to the United States.28 The U.S. uses over 20.7 million barrels a day of crude oil and products and imports 58.4% of that requirement.29 On 19 January 2006 al-Qaeda leader Osama bin Laden announced in a video release that, “The war against America and its allies will not be confined to Iraq…..”, and since June of 2003 there have been 298 recorded attacks against Iraqi oil facilities.30 Terrorists conduct research as to the easiest point to damage the flow of oil or to the point where the most damage can be done. Scenarios involving the oil fields themselves, a jetliner crashing into the Ras Tanura facility in Saudi Arabia could remove 10 percent of the world’s energy imports in one act.31 Maritime attacks are also option for terrorists; on October 6, 2002 a French tanker carrying 397,000 barrels of crude oil from Iran to Malaysia was rammed by an explosive laden boat off of the port of Ash Shihr, 353 miles east of Aden. The double-hulled tanker was breached, and maritime insurers tripled the rates.32 Energy most travel often long distances from the site where it is obtained to the point where it is converted into energy for use, a catastrophic event at any of the sites or along its route can adversely impact the energy infrastructure and cause ripples in other infrastructures. The security of the pipeline in Alaska increases in importance as efforts are made to make America more independent on energy use.

Economy

The U.S. economy is the end-state target of several terrorist groups as identified in the introduction quote. The means by which terrorists and other threats attempt to impact the economic infrastructure is through it’s linkage to the other infrastructures. Attacks are launched at other infrastructures, such as energy or the Defense Industrial Base in an effort to achieve a “cascading” result that impacts the economy. Cyber attacks on Banking and Finance are another effort to indirectly impact the economy. The short term impacts of the 9/11 attacks on Lower Manhattan resulted in the loss of 30% of office space and a number of businesses simply ceased to exist. Close to 200,000 jobs were destroyed or relocated out of New York City. The destruction of physical assets was estimated in the national accounts to amount to $14 billion for private businesses, $1.5 billion for state and local government enterprises and $0.7 billion for federal enterprises. Rescue, cleanup and related costs are estimated to at least $11 billion for a total direct cost of $27.2 billion.33 The medium and long term effects cannot be accurately estimated but demonstrate the idea of cascading effects. The five main areas affected over a longer period were Insurance, Airlines, Tourism and other Service Industries, Shipping and Security and military spending. At various times terrorist rhetoric has mentioned attacks against Wall Street proper, but the more realistic damage to the economy will come through the indirect approach of cascading effects.

Transportation

The attack on commuter trains in Madrid in March of 2004 and the London bombings in July of 2005, which together killed 243 people, clearly indicated the threat to the transportation infrastructure. Statistics provided by the Brookings Institute in Washington DC show that between 1991 and 2001 42% of worldwide terrorist attacks were directed against mass transit. Transportation is viewed by terrorists as a “soft target” and one that will impact the people of a country. Mass Service Transportation (MST) is the likely target of a terrorist attack.

MST caters to large volumes of people, crammed into narrow confined spaces

MST is designed to move large numbers of people quickly and efficiently, which is often counter to protective measure

MST assets are enclosed, serving to amplify explosions

MST attacks can result in “cascading effects” because communications and power conduits are usually collocated in proximity to their routes

The Department of Homeland Security sent a “public sector notice” in May of 2006 based on two incidents of “suspicious videotaping” of European mass-transit systems.34 The individual had several tapes besides the one in his camera, none of which showed any tourist sites. The tapes focused on the insides of subway cars, the inside and outside of several stations and exit routes from the stations. In June of 2003 the FBI arrested Iyman Faris, a 34 year old naturalized American citizen who had been in contact with Al Qaeda conducting research and reconnaissance in an effort to destroy the Brooklyn Bridge.35 Mr. Faris had traveled to Afghanistan and Pakistan in 2000, meeting with Osama bin Laden, he returned to the U.S. and began gathering information concerning the Brooklyn Bridge and communicating via coded messages with Al Qaeda leaders. An attack on the bridge would have not only damaged the transportation infrastructure, but also a known American landmark. On 24 May 2006, a Pakistani immigrant was convicted on charges of plotting to blow up one of Manhattan’s busiest subway stations in retaliation for the U.S. actions at the Abu Ghraib prison.36

Terrorist threats to the transportation infrastructure extend beyond land to the sea. Vice Admiral Jonathan Greenert, commander of the U.S. Seventh Fleet, said “one of my nightmares would be a maritime terrorism attack in the Strait of Malacca”.37 “There is a strain of al-Qaida in Southeast Asia, called Jemaah Islamiya. They are actively pursuing a maritime terrorism capability that includes diving and mining training.”38 As how this might impact on the economy, $220 billion in trade comes through the Seventh Fleet area of responsibility and 98% of the commerce is moved by sea. Just as ports can be viewed a SPOF within the maritime transport system, there are certain waterway chokepoints or heavily trafficked areas that can be viewed as a high payoff target to a terrorist or result in catastrophic damage from a natural disaster.

#### Extinction.

Liu '18 [Qian; 11/13/18; Managing Director of Greater China for The Economist Group, previously director of the global economics unit and director of Access China for the Economist Intelligence Unit, PhD in economics from Uppsala University; "The next economic crisis could cause a global conflict. Here's why," <https://www.weforum.org/agenda/2018/11/the-next-economic-crisis-could-cause-a-global-conflict-heres-why/>] // Re-Cut SJWen

The next economic crisis is closer than you think. But what you should really worry about is what comes after: in the current social, political, and technological landscape, a prolonged economic crisis, combined with rising income inequality, could well escalate into a major global military conflict. The 2008-09 global financial crisis almost bankrupted governments and caused systemic collapse. Policymakers managed to pull the global economy back from the brink, using massive monetary stimulus, including quantitative easing and near-zero (or even negative) interest rates. But monetary stimulus is like an adrenaline shot to jump-start an arrested heart; it can revive the patient, but it does nothing to cure the disease. Treating a sick economy requires structural reforms, which can cover everything from financial and labor markets to tax systems, fertility patterns, and education policies. Policymakers have utterly failed to pursue such reforms, despite promising to do so. Instead, they have remained preoccupied with politics. From Italy to Germany, forming and sustaining governments now seems to take more time than actual governing. And Greece, for example, has relied on money from international creditors to keep its head (barely) above water, rather than genuinely reforming its pension system or improving its business environment. The lack of structural reform has meant that the unprecedented excess liquidity that central banks injected into their economies was not allocated to its most efficient uses. Instead, it raised global asset prices to levels even higher than those prevailing before 2008. In the United States, housing prices are now 8% higher than they were at the peak of the property bubble in 2006, according to the property website Zillow. The price-to-earnings (CAPE) ratio, which measures whether stock-market prices are within a reasonable range, is now higher than it was both in 2008 and at the start of the Great Depression in 1929. As monetary tightening reveals the vulnerabilities in the real economy, the collapse of asset-price bubbles will trigger another economic crisis – one that could be even more severe than the last, because we have built up a tolerance to our strongest macroeconomic medications. A decade of regular adrenaline shots, in the form of ultra-low interest rates and unconventional monetary policies, has severely depleted their power to stabilize and stimulate the economy. If history is any guide, the consequences of this mistake could extend far beyond the economy. According to Harvard’s Benjamin Friedman, prolonged periods of economic distress have been characterized also by public antipathy toward minority groups or foreign countries – attitudes that can help to fuel unrest, terrorism, or even war. For example, during the Great Depression, US President Herbert Hoover signed the 1930 Smoot-Hawley Tariff Act, intended to protect American workers and farmers from foreign competition. In the subsequent five years, global trade shrank by two-thirds. Within a decade, World War II had begun. To be sure, WWII, like World War I, was caused by a multitude of factors; there is no standard path to war. But there is reason to believe that high levels of inequality can play a significant role in stoking conflict. According to research by the economist Thomas Piketty, a spike in income inequality is often followed by a great crisis. Income inequality then declines for a while, before rising again, until a new peak – and a new disaster. Though causality has yet to be proven, given the limited number of data points, this correlation should not be taken lightly, especially with wealth and income inequality at historically high levels. This is all the more worrying in view of the numerous other factors stoking social unrest and diplomatic tension, including technological disruption, a record-breaking migration crisis, anxiety over globalization, political polarization, and rising nationalism. All are symptoms of failed policies that could turn out to be trigger points for a future crisis. Voters have good reason to be frustrated, but the emotionally appealing populists to whom they are increasingly giving their support are offering ill-advised solutions that will only make matters worse. For example, despite the world’s unprecedented interconnectedness, multilateralism is increasingly being eschewed, as countries – most notably, Donald Trump’s US – pursue unilateral, isolationist policies. Meanwhile, proxy wars are raging in Syria and Yemen. Against this background, we must take seriously the possibility that the next economic crisis could lead to a large-scale military confrontation. By the logic of the political scientist Samuel Huntington , considering such a scenario could help us avoid it, because it would force us to take action. In this case, the key will be for policymakers to pursue the structural reforms that they have long promised, while replacing finger-pointing and antagonism with a sensible and respectful global dialogue. The alternative may well be global conflagration.

## 2

#### Interp: Debaters must provide at trigger warning before round

#### Violation: they didn’t

#### Standards – exempted

## Case