

# Cyberwar: The ISIL Threat

&

# Resiliency in Operational Technology

---

Thesis Presented to  
the Faculty of the Department of  
Information and Logistics Technology  
University of Houston

---

In Partial Fulfillment of  
the Requirements for the Degree  
Master's of Information Systems Security

---

By  
Gregory S. Anderson  
May 2017

Cyberwar: The ISIL Threat  
&  
Resiliency in Operational Technology

---

Gregory S. Anderson

Approved:

Committee Chair: \_\_\_\_\_

Wm. Arthur Conklin, PhD  
Computer Information Systems and  
Information System Security

Committee Member: \_\_\_\_\_

Chris Bronk, PhD  
Computer Information Systems and  
Information System Security

Committee Member: \_\_\_\_\_

Paula deWitte, PhD  
Computer Information Systems and  
Information System Security

---

Rupa Iyer, PhD

Associate Dean for Research and Graduate  
Studies, College of Technology

---

Dan Cassler

Interim Chair for Department of Information  
and Logistics Technology

THIS PAGE  
INTENTIONALLY  
LEFT BLANK

## Acknowledgments

First, I would like to thank Dr. Chris Bronk and Dr. Art Conklin for their support and guidance throughout my time at the University of Houston. Their dedication to students is unparalleled for any other professor I have come across during my education.

I would also like to thank my family for their ongoing encouragement and love. The fostering environment to peruse knowledge and “never settle for less” has been a constant inspiration throughout my life.

Lastly, to my partner of 7 years, Lorelei. None of my achievements these past few years would have come to fruition without her continuous love, support, and willingness to sacrifice for the greater good is deeply appreciated. Thank you for being the most patient and steadfast person I have ever known, I love you.

# Cyberwar: The ISIL Threat

## Table of Contents

Introduction.....	2
Contemporary Counter Insurgency Operations in the Middle East.....	3
An Appraisal of Contemporary Cyber Operations .....	6
Why They Fight – ISIL Social Media & Propaganda.....	11
ISIL’s Cyber Capabilities and Intent .....	15
The ISIL Cyber Complex.....	18
Policy Options – Cyber Offense Against ISIL .....	21
Glossary of Abbreviations .....	26
References .....	28

## Introduction

Although the United States withdrew its last remaining significant military forces from Iraq in December 2011, a significant insurgency spanning the territory of Iraq and Syria has evolved under a variety of names including the Islamic State, Islamic State in Syria (ISIS) and the Islamic State in Iraq and the Levant (ISIL). (For the purposes of this work, we choose to employ the title ISIL.) Since its inception coming on the heels of a break with the al-Qaeda in February 2014, it has come to be the chief standard bearer of a Salafi Jihadist movement set upon forming a trans-regional caliphate. In its activities, ISIL has extended its territorial reach across North Africa and the Arabian Peninsula as well as claiming credit for terror attacks from Belgium to Bangladesh. As much as a movement, ISIL is the contemporary brand for Jihadist insurgency in the Middle East and beyond.

While ISIL forces have made impressive territorial gains in Iraq and maintained a viable resistance to the Assad government in Syria, it is now extending its reach into the digital domain, cyberspace, to further its ambitions in intelligence collection, propaganda, and recruitment. In addition, ISIL is perhaps the first violent insurgent or terror group to seriously consider developing at least modest cyber-attack capabilities as well as developing strength in sophisticated computing and communications technologies designed to defend the identity of its adherents and the security of their digitally-mediated interactions. (Paganini, 2015)

For the United States, the fight against ISIL also represents a significant test of its own offensive cyber capabilities. Yes, ISIL has put US forces on the defensive, but if Cyber Command (CyberCom) is to be a viable part of the Department of Defense's mix of forces going forward, it will need to demonstrate how it can be of utility in the counter-insurgency and counter-terrorism

struggle against ISIL and its confederates. The fight against ISIL will represent a significant test of how CyberCom can operationalize tactical capabilities in line with strategic goals on marginalizing and eventually defeating this organization.

Provided here are observations of ISIL cyber power, from digital information operations and intelligence, to operational security and desired future capabilities. We also examine openly available reporting on US cyber operations against ISIL and declarations of leadership intent from the Defense Department and national leadership here in the United States. Finally, we offer a prescriptive component which mates desired outcomes for diplomatic activities and military operations aimed against ISIL in the US Central Command area of responsibility with cyber options, both known and desired.

## Contemporary Counter Insurgency Operations in the Middle East

Although ISIL's roots are tied to the al-Qaeda terror organization, it has embarked upon a far more ambitious agenda for Islamic statehood that combines previous operational tradecraft in terror operations with a clear desire to capture and hold significant territory and generate economic activity sufficient to challenge state authority in its primary operating theater – Iraq and Syria. Combat operations against ISIL by outside military forces, including those of Iran, the United States (along with coalition allies), and Russia began in the summer of 2014. Russia deployed its contingent of air and ground forces to Syria in 2015, however. Fighting against ISIL has created a coalition of rather unusual bedfellows.

Iran, a traditional foe of the United States since the 1979 Revolution, has a significant stake in supporting the coalition government of Iraq, with its large representation of Shia political leaders. (Nader, 2015) To this end, it has provided both air power and advisers on the ground to



forces of the Iraqi army and pro-government militias. In parallel with the Iranian intervention, the United States has gradually reintroduced forces into Iraq, a number which stands at 4,650 as of July 2016. In addition to advisers and logistical support, the US maintains significant numbers of manned and unmanned aircraft in the region that have been employed in intelligence, surveillance and reconnaissance (ISR) missions as well as air strikes against ISIL forces. Russia's involvement appears confined to Syria, in the form of air power and limited numbers of ground forces. Russia has also aided autonomous Kurdish forces in Syria. (Grove & Kesling, 2016)

The Kurdish dimension to the ISIL conflict in Iraq and Syria further broadens the set of interested parties, most significant among them, Turkey. Considerable US and coalition resources have gone into supporting Kurdish military forces in Iraq. While the Iraqi Army collapsed in the face of the 2014 ISIL offensive, Kurdish troops have been viewed as more effective in protecting territories viewed as their own, but they are not without internal issues. (Gonzalez, 2015) In addition, Iraq's current president, Fuad Masum, is an ethnic Kurd. While the interplay of Iraqi internal politics is of limited salience here, the Kurdish issue and the threat it presents to Turkey produces interesting information or possible cyber geopolitics relevant to the conflict as the Erdogan government has routinely found issue with the actions of its internal opponents on social media. (Taylor, 2014)

Military operations against ISIL undertaken by the US-led coalition cohere well with the form of conflict summarized by now-retired admiral James Stavridis, the former commander of US forces in Europe. His view of contemporary conflict and that of the near future is that it will be dominated by drones, special operations forces (SOF), and cyber. (Stavridis, 2013) And to a great degree, that is the force mix that the US and its allies have fielded in Iraq and, to a lesser degree, Syria. Besides the US, Australia, Canada, Denmark, Germany, New Zealand, Norway,

Spain, and the United Kingdom have deployed ground contingents, primarily composed of military advisers in Iraq and/or Iraqi Kurdistan. Many of these troops are the same sort of special operations forces called upon for direct action operations aimed to rescue hostages, identify targets for precision munitions, or neutralize ISIL leadership targets.

The other highly visible activity in counter-ISIL operations is air power. The preferred method by which both Russian and coalition power has been operationalized in the theater is through air strikes and drone attacks. Among the US-led coalition in conducting air strikes has been Arab nations including Jordan, Morocco, and the United Arab Emirates. “The campaign against ISIS cannot be won by airpower alone.” (Eisenstadt, 2014) While it can be and likely has been useful in breaking up large concentrations of ISIL ground forces, it is less so as ISIL goes to ground. As former MI6 officer and EU adviser Alastair Crooke observed, air strikes, “are more likely to kill people who are not involved because the practice of these groups is to break up their formations, dissipate and then move on to built-up areas and hide within the populations.” (Moore, 2015)

Then there are the concerns for spillover of the conflict into neighboring countries, including Turkey, Saudi Arabia, and Jordan. With a lengthy land border with Iraq and Syria as well as its own concerns regarding its Kurdish minority, Turkey has much to fear regarding Islamic terrorism on its soil as well as strong Kurdish militaries in its neighbors. Less a factor in counter-ISIL operations has been Saudi Arabia, which has worked to train token numbers of fighters for operations in Syria. However, the Kingdom has been a recent target of violence by ISIL confederates in recent months, including at its holiest sites, including Medina. (Dabashi, 2016) Finally, Jordan, which hosts more than a million Syrian refugees on its territory, is already stretched thin in extending its national resources to provide for them.

While this brief geopolitical overview of the core ISIL Iraq-Syria theater of operations is hardly detailed, it is necessary to have at least some understanding before considering either ISIL's cyber operations or those operations directed against it. In addition to understanding the geopolitics, it is also important to briefly assess the recent record of information and cyber operations undertaken beyond the scope of the ISIL conflict.

### An Appraisal of Contemporary Cyber Operations

At a number of points in the last decade, cyber operations gradually moved from being an area of the imagination to a viable option for states and non-state actors. (Bronk, 2016) The record of cyber-attacks has grown gradually as different actors have demonstrated the will and capacity to make use of techniques and tools that compromise, manipulate, and damage information systems held by both governments and private entities. A politics of cyber action, hacktivism, draws upon older traditions of civil disobedience and non-violent protest. (Olson, 2013) Such activities are often conceived of or conceptualized as David versus Goliath struggles against powerful public and private organizations.

When we consider cyber actions with real impact upon organizations, however, the record of major events thins out considerably. For years, the only openly known or discussed incident of a cyber-attack with producing a significant physical outcome spoken about by officials of the US government and Intelligence Community (IC) was the insider attack by a disgruntled software engineer upon the Australian municipality of Maroochy Shire. (Brenner, 2013) Stuxnet, the malware attack against Iran's nuclear enrichment infrastructure, represented a crossing of the Rubicon when it was discovered by security researchers in the summer of 2010. (Segal, 2016) It made real the threat of cyber-attacks on critical infrastructure such as petrochemical plants, the

electrical grid, manufacturing facilities, oil and gas wells, and nuclear power stations. Stuxnet was the world's first view into what a cyber-attack with kinetic impact looked like. (Applegate, 2013)

Three years before Stuxnet, the Baltic nation of Estonia became the first country to face a comprehensive cyber campaign directed against its digital infrastructure. The cyber-attacks on Estonia in April and May 2007 were triggered by displeasure in Russia and within Estonia's Russian minority regarding the move of the memorial to the unknown dead of the Great Patriotic War (World War II) from a site in downtown Tallinn to a military cemetery outside the city center. The cyber-attacks against Estonia were of little military value, but they did demonstrate the degree to which anti-Estonian hackers, with or without sanction from Moscow, could make life difficult in the highly "wired" former republic of the Soviet Union. (Waterman, 2007)

Since the Estonia episode, there has been a rise in cyber operations by many of the world's most significant powers. Russia has continued to integrate a cyber component into its geopolitical dealings, using cyber means not only to collect intelligence but also shape the information landscape surrounding its political, military, and economic interests. (Heickerö, 2010) When Russia engaged in military operations against Georgia in 2008, cyber capabilities were again leveraged in a manner similar to those in Estonia, but in advance of, and simultaneously with, a significant military intervention involving the ground, air, and naval forces of the Russian state. Since Georgia, Russia has developed the capability to launch, "highly coordinated disinformation campaign[s]," that blur the boundary between information warfare and the nefarious trolling of individuals and organizations that has become a hallmark of the Internet's deeply dysfunctional ecosystem. (Chen, 2015)

Russia's intelligence services have adopted cyber tools and techniques to further the country's interests as well. The Russians are alleged to have compromised computer systems in the State Department, in the Department of Defense, and at the White House. Buckshot Yankee was also a significant cyber event in which the classified secret-level computer systems of US forces in Afghanistan were compromised by malicious software (malware), ostensibly from a Russian source. Russia also conducted the requisite reconnaissance and preparation to enable targeting of computer systems employed in operation of critical infrastructure and heavy industry. The West's major oil and gas companies' industrial control systems were extensively probed in a cyber campaign dubbed *Energetic Bear*. (Pagliery, Russia Attacks U.S. Oil and Gas Companies in Massive Hack, 2014) More recently, when the Ukrainian electrical grid was seriously disrupted by a well-prepared cyber-attack, Russia was considered to be the most likely culprit. Russia's cyber intelligence operations are widely considered to be well-organized, expertly executed and very stealthy in nature. That is not necessarily the case for the other major threatening nation state to the US and its allies with regard to cyber-attack.

Where Russia's cyber capabilities have extended into hacks against physical infrastructure, the People's Republic of China have thus far been more oriented at the collection of intelligence. Chronicled in the APT 1 report produced by security consultancy Mandiant, China's early Advanced Persistent Threat campaigns were viewed as effective, but also fairly primitive in tradecraft and "noisy", in that the perpetrators appeared to do little to cover their tracks or eliminate evidence of their presence on compromised networks. (Mandiant, 2013) Nonetheless, China has become more effective in its cyber-attack capabilities. (FireEye, 2016) The compromise of the US Office of Personnel Management's employee database (which extended to prospective employees and other individuals tied to federal workers) can be considered China's triumph in

gaining deep inside knowledge of the US federal workforce, including hundreds of thousands of employees and contractors holding various levels of security clearance regarding classified information.

The United States has been a frequent target, but is also generally regarded as a highly-sophisticated player in cyber intelligence and offensive cyber action capabilities. (Beene, 2016) In the wake of the Stuxnet revelation, analysts in Iran and Russia uncovered other pieces of malware likely created by the US and/or its allies. Russian security firm Kaspersky labeled the authors of this software, the *Equation Group*. (Kaspersky Lab, 2015) Documents made public by Edward Snowden further illuminated the sophisticated cyber intelligence collection capabilities developed by the National Security Agency (NSA). (MacAskill & Dance, 2013) The Snowden documents underscore a well-developed idea that the cyber capabilities of The Five Eyes allies (Australia, Canada, New Zealand, UK, and US) surpass those of any other countries on the planet.

While the US, Russia, and China may be the world's most significant cyber powers, both lesser nation states and groups not aligned with individual countries also matter. Two incidents underscore the growth in the former group; the 2012 cyber-attack against Saudi Aramco and the 2012 breach at Sony Pictures Entertainment. Both incidents, generally attributed to Iran and North Korea respectively, offer examples of how smaller, more resource-constrained nation states may employ cyber techniques to serve their international interests. (Shamah, 2014)

Because the barriers to entry for engaging in cyber espionage and covert action can be quite low, non-state actors have employed cyber tools to express beliefs and exert influence. While the beginnings of such activity reach back to 'hacktivist' activities in the 1990s, a distinct form of political computer hacking organization has evolved under the banner of the Anonymous

organization since its inception in approximately 2004. Anonymous and related organizations, LulzSec and AntiSec, have implemented hacking as dissent or societal criticism in the collective consciousness of Western society. (Coleman, 2014) The activities of Anonymous or its confederates provide a blueprint for groups that espouse values at odds with traditional models of state or corporate power. It is a group that is activist in nature that employs a repertoire of computer hacking to exert influence. In describing itself, Anonymous has said it's "a very loose and decentralized command structure that operates on ideas rather than directives." (Kelly, 2012)

Organizational definitions aside, much can be understood of Anonymous by who or what it chooses to target and why. The group came to some prominence in the US for its activities in opposition to the Westboro Baptist Church, the Church of Scientology, the State of Arizona (for S.B. 1070, a controversial piece of immigration legislation), the Bay Area Rapid Transit system (for its role in attempting to suppress protests in San Francisco), and Aransas County, Texas, as well as by supporting the Occupy protests across the United States.

In addition to Anonymous, the WikiLeaks organization has eschewed hacking activities to instead serve as a repository for public visibility of proprietary or controlled information. Although the group's de facto figurehead, Julian Assange, remains voluntarily sequestered in the Ecuadorean embassy to the United Kingdom, it continues to host documents not necessarily for public consumption. (Alexander, 2016) The most recent archive of note being a set of emails apparently purloined from the US Democratic National Committee (DNC), possibly by Russian hackers. (Fisher, 2016) WikiLeaks' actions are important to understanding the larger information conflict that is embedded in contemporary geopolitics. (Deibert, 2015) Whether the Manning archive of State Department cables or the DNC emails, WikiLeaks has stood by a decision to make public all that it receives.

These documents, and other leaked archives, including the “Panama Papers” of law firm Mossack Fonseca leaked to a German newspaper and then passed to the International Consortium of Investigative Journalists (ICIJ), have likely had significant impact on both international and domestic politics. (Birchall, 2014) They are a delegitimizing force even in democratic societies as they demonstrate at least the unvarnished realities of politics and at worst the significant corruption still present even at the highest levels in many governments. If ISIL can penetrate similar targets to meet its strategic objectives, it may well try to do so. The breach of the Saudi Foreign Ministry’s communications system in July 2015 is an indicator of how hackers or internal leakers can threaten regimes in the Middle East. The Saudi messages revealed a record of, “putting foreign preachers on the Saudi payroll, building mosques, schools and study centers, and undermining foreign officials and news media deemed threatening to the kingdom’s agenda.” (Hubbard & Sheikh, 2015) But ISIL’s primary use of the Internet, an information weapon if not a cyber one, is recruitment of fighters, including thousands of foreigners, to its cause, not only in the Levant, but also the greater Middle East.

## Why They Fight – ISIL Social Media & Propaganda

Use of social media to distribute Jihadist messages arose almost as quickly as the technology was invented. In the hands of Jihadist groups, it is an outgrowth of a socially-mediated network in which messages were passed on video and audiotape, each copied and recopied at each intermediate point in its path across the Middle East and beyond. Videotapes of hostages (usually Western) were popular and were employed to sending a message of strength and opposition. Where these videos were once used to demonstrate proof of life, after 9/11, Abu Musab al-Zarqawi and other al Qaeda leaders released execution videos of hostages. The videos created controversy



due to their harsh brutality, and this has since become a staple for ISIL propaganda. (Yan, 2014) These videos increased significantly in 2014 when ISIL officially parted ways with al Qaeda and showed footage of the beheading of American journalist, James Foley. ISIL pushes this type of media through its own online sites as well as major American platforms, including YouTube and Twitter.

To help understand the narrative that ISIL is trying to construct, it is pertinent to understand the medium it attempts to master. In order to maximize exposure for their propaganda related activities, ISIL has maintained a heavy presence on social media platforms including Twitter, Instagram, and YouTube. While the Twitter platform is not built for sustained diatribes, their brief 140 character updates allow for a constant flow of reinforcement. Instagram represents another vehicle for propaganda distribution available to ISIL and represents a useful image-based complement to Twitter. (Webb, 2015) Instagram's primary function is sharing videos and pictures. The proliferation of high quality cell phone cameras and Go-Pro type lightweight mobile cameras, allows ISIL to share, in morbid detail, their most violent exploits with just a few clicks. (Zero Censorship, 2016) These activities plainly violate the terms of service of these sites, and both Twitter and Instagram have taken steps to stop the spread of ISIL propaganda, including, but not limited to, blocking known ISIL accounts. (Goldman, Twitter goes to war against ISIS, 2016)

ISIL is uniquely positioned in its use of the Internet in a manner that allows them to reach across the world and "become pen pals with a lonely teenager in small-town America." (Singer & Brooking, 2015) Not only are their social media attempts to recruit fence-sitters and sympathizers to travel to the Middle East or carry out their own terror attacks in their home country, they are trying to provoke the West into sending troops to take on ISIL on the ground. By provoking a

military response out of the United States and its allies, ISIL can play a victim and continually reinforce the claim that “the West is engaged in a crusade against Muslims.” (Blanchette, 2016)

The organization has successfully made full use of so-called ‘viral’ marketing campaigns to establish itself on the Internet. It has created a brand for itself, networked with other terrorist groups, and engaged with their supporters through social media. (Singer & Brooking, 2015) Through this media campaign they have been able to recruit from around the world. An example is Usaamah Rahim of Boston, Massachusetts, who sought to kill police officers. (Almasy, 2015) Rahim was radicalized to some degree in correspondence via the Internet and expressed sympathies for the Islamic State on social media. (Sanchez, 2015) As with al Qaeda before it, ISIL has a well-staked interest in radicalizing persons already in the United States and other Western countries to the point that they are willing to engage in terror attacks. These individuals, exemplified by San Bernardino shooters Rizwan Farook and Tashfeen Malik, who often operate alone or in small, but very tightly knit groups, represent the most replicable of assets for ISIL to strike at targets beyond the Middle East. Another propaganda call is for adherents to the ISIL cause to travel to the Middle East for training and participation in military action in Iraq, Syria, or other operational areas.

As of late August 2014, “as many as 3,000 Westerners” had been recruited and were fighting alongside ISIL and related Jihadist groups in Syria and Iraq. (CBS News, 2014) ISIL has constructed a sophisticated online media machine that has been masterfully crafted for the purposes of recruiting Westerners. One such wing of this activity is the Al Hayat Media Center, which was established in May of 2014. Al Hayat publishes in a variety of languages, including French, German, and English. Most of the content that is posted is in English, which strongly “suggests that they are specifically designed as a recruitment tool for Western audiences.”

(Becker, 2014) One of the programs run by Al Hayat is called mujatweets (mt), which showcases the group's domestic efforts of winning support by showing the "lighter side of life in ISIS." One example of this is called "Cats of Jihad," in which ISIL fighters pose cats with their weapons. (Singer & Brooking, 2015)

The U.S State Department has estimated that roughly 12,000 foreigners from 50 different countries have traveled to Syria to fight with ISIL, most of which are considered youth (age 15 to 25). (Trianni & Katz, 2014) Of those 12,000 foreign ISIL fighters, it is estimated that roughly a third are from Western countries. (Callimachi, ISIS and the Lonely Young American, 2015) As mentioned previously, ISIL tends to focus their recruiting efforts towards Western youth (as made evident by the high amount of English propaganda). ISIL recruiters discern if potential recruits are more likely to carry out terrorist attacks in the recruit's home country or if they'll join ISIL in the Middle East. It's the job of the recruiters to create an online community to encourage the recruit to break ties with any outside channel that could disrupt the recruitment process (e.g. family and friends). (Haq, 2014) Many of those recruited become expendable cannon fodder and are encouraged to further the brutal propaganda campaign by creating videos and "blowing themselves up." (Hall, 2015)

The recruits that do not head to Syria or Iraq, are strongly encouraged through the online ISIL community to carry out terrorist attacks in their home country. As the organization has said of the West, "the tiniest action you do in the heart of their land is dearer to us than the biggest action by us. There are no innocents in the heart of the lands of the crusaders." (The Guardian, 2016) Online recruiters offer guidance on how to carry out an attack and offer resources on how to construct or acquire materials if necessary. Lone Wolves in the West are considered a relatively cheap resource for ISIL. If a Lone Wolf carries out a terrorist attack, ISIL can choose to claim

credit or not, depending on its outcome. Lone Wolves are also incredibly useful as they typically use their own financial resources to carry out attacks.

## ISIL's Cyber Capabilities and Intent

While the Internet has served as an important vehicle for recruiting adherents to Jihadist causes, the US and its allies will need to prepare for ISIL's expanding capabilities and those of its successors. Recruitment is but one measure of ISIL's power. There are many others, including its financial resources, capacity to communicate at a distance, ability to plan and execute coordinated operations, and acquire increasingly sophisticated armaments and use them effectively in traditional and unconventional combat operations.

ISIL has also made liberal use of Facebook Groups to conduct arms trafficking, including the sale and transfer of small arms and other munitions. (Chivers, 2016) These Facebook groups very closely mimic legal American counterparts with the open posting of ads with pictures, descriptions, and prices for everyone to see. Transactions are then presumably carried out in person. However, Facebook's terms and policies updated in late January 2016 have disallowed all open trading of firearms and other munitions for all users regardless of country or affiliation. (Guynn, 2016) Unfortunately, Facebook relies heavily on the user to report violations of these terms.

ISIL and other groups aligned with it have also started moving secure activities to other social media websites such as Diaspora. (Lee, 2014) Diaspora is a decentralized social network with data stored on private servers (called pods) that are not controlled by Diaspora's staff. This leaves the removal of ISIL (and ISIL-related) content up to the owner of the pod. Due to the design of these platforms, the dispersal of propaganda material does not match that of Twitter and

Instagram. However, it does users to operate with more impunity. In addition, ISIL appears to be wising up on digital operational security. Although many of the group's operations have employed open, unencrypted communications, a group at West Point's Combating Terrorism Center located a 34-page operational security manual. Initially drafted by a Kuwaiti firm as advice for journalists and activists in Gaza, the document has been employed as a primer by ISIL as well. (Zetter, 2015)

Despite social media sites attempts at preventing the spread of ISIL imagery, news, and other content, they are operating within the watchful eye of the world in most forms of commonly accessed social media. America's long history of trying to 'win the hearts and minds' of foreign publics in counterinsurgency operations stretches back as far as the Philippine-American War. ISIL recognizes the ideological struggle with the US and is able to employ the Internet as perhaps its most valuable outlet for promoting narratives useful to the organization in public view. With regard to combat operations, this places US and coalition forces in a precarious position, just as insurgencies can wreak havoc to an organized force with strictly enforced rules of engagement, the fight against ISIL adds the additional concern of a global audience to be witness to any misstep by coalition forces that result in collateral damage and civilian fatalities. Finally, ISIL also has coordinated attacks and intimidated enemy forces into giving up, due to its overarching information operations. This was the case when some 1,500 ISIL fighters took control of Mosul from some 30,000 Iraqi soldiers and police in June 2014. ISIL has been effective in its use of social media, and has quickly adapted to bring further support for their cause.

ISIL has so far proven itself very adaptable to the changing terror environment by seeking new ways to impose its Jihad on the West. For now, these attacks have largely remained juvenile in nature. In a few cases, they have gained access to Twitter feeds of military officials involved in operations in the Middle East or in defacing websites regarding military spouses. (Marks, ISIL

Aims to Launch Cyberattacks on U.S., 2015) These attacks have largely remained inconsequential to any military operations but it must be seen as the early steps into incorporating a proper cyber offensive. Furthermore, ISIL has already been spotted online talking openly about the possibilities of hacking into aviation instruments of large passenger planes to wreak havoc on those aboard as well as the possibility of using attacks to infiltrate Western nuclear power plants to release deadly radiation into the country side. (Mchugh, 2015) While these fears have yet to be realized, ISIL has already begun the initial stages of intrusion into our electrical grid. (Pagliery, ISIS Is Attacking the U.S. Energy Grid (and Failing), 2015) These attacks have been entirely unsuccessful and low level in nature, however it paints a clear picture to the intent of ISIL. The attacks themselves were mostly executed by basic attack software that can be purchased through online dark net market websites such as the Silk Road and its successors. By using social media, ISIL seeks to gain guidance to internally produce malware to carry out these attacks while also accessing code produced by hackers for hire.

Additionally, it can be assumed that ISIL will make better use of bot software to more effectively spread their message through Twitter. (Goldman, Twitter Goes to War against ISIS, 2016) Currently, the traditional system of making thousands of accounts to swarm feeds and hashtags, both items that increase message visibility, is being countered by tactics taken by Twitter. However, new apps (such as the Android app The Dawn of Glad Tidings) are being built that allow predetermined messages written by ISIL social media coordinators to be slowly spread by users with real accounts who choose to opt-in. (The Atlantic, 2014) When a user chooses to opt-in, their account functions normally most of the time, but it will periodically broadcast tweets from ISIL that are sent around at the same time to thousands of other accounts. (CBS DC, 2014) These

accounts are difficult to detect and allow for users who already have large amounts of followers to get their message out.

Usage of the app even varies the timing of posts that are made to minimize detection but to maximize exposure during offenses. During the offensive launched into Mosul, the ISIL controlled accounts sent out over 40,000 tweets. (Cuthbertson, 2014) ISIL has recognized the new threat network that advanced attacks on United States systems can provide through cyber warfare and we need to do the same.

## The ISIL Cyber Complex

We are aware that ISIL can and will conduct cyber warfare operations, a significant threat to US interests. Through cyber operations, ISIL's sphere of influence is further extended from Iraq and Syria. As mentioned previously, ISIL has already indicated making cyber-attacks against critical infrastructure targets, including the US electrical grid. Unlike cyber-attacks from China, Iran, and Russia, ISIL hackers are more devoted to their cause as they are actively engaged in hostilities against the US and its allies. ISIL cyber capabilities are not on par with those of major adversary nation-states, but the determination of the organization can be found in the exploits of two ISIL-aligned computer hackers: Junaid Hussain and Ardit Ferizi. Neither Hussain's nor Ferizi's origins are in Syria or Iraq, but rather Europe.

Junaid Hussain rose to prominence in Middle Eastern hacking circles in 2011, when he compromised the digital address book and personal accounts of former UK prime minister Tony Blair. Using the hacker handle, TriCk, he was just 17 years old when British authorities jailed him. Hussain, a British-born hacktivist turned pro-ISIL hacker of Pakistani descent became involved with TeaMp0isoN, an Islamic hacking organization, contributing to the group's efforts.

Other members of the TeamP0ison hacking group reputedly overloaded MI6's counter-terror hotline later that year. Politicized through watching videos of violence against children in Palestine and Kashmir, Hussain told an interviewer of his motivations in 2012: "I wanted to know why this was happening and who was doing it, there was loads of questions in my head. It made me angry, it changed the way I lived my life and the way I saw the world. I then started using hacking as my form of medium by defacing sites to raise awareness of issues around the world and to 'bully' corrupt organizations and embarrass them via leaks etc., which is how I got into hacktivism." (Murphy, 2015)

Upon release, Hussain made his way to Syria with his British wife, a convert to Islam, and set to work on training others in the ISIL organization the tradecraft he had developed before his six-month stint in prison. He was an associate of Mohammed "Jihadi John" Emwazi, the ISIL spokesperson known for his role in the killing of Western hostages James Foley and Steven Sotloff. Hussain produced results for ISIL. In Syria, he and his confederates hacked the Twitter and YouTube accounts of US Central Command, which oversees operations of forces across the Middle East and Southwest Asia. (Francecshi-Bicchierai, 2015) More threatening was how Hussain employed a technique known as "doxing" to build dossiers of personally identifiable information found online regarding US and allied service members and their families. (Garber, 2014) The capacity for ISIL digital operatives to pass such information along to confederates in the United States or Western Europe willing to attack relatively soft targets is a serious concern.

For some time, scholars of the law of armed conflict have considered the question of when a nation-state would meet a cyber-attack with a kinetic response. The killing of Junaid Hussain in an August 24, 2015 US airstrike in Syria appears to have answered that question. In killing Junaid Hussain, the Pentagon displayed a capacity to meet cyber power with kinetic force. It appears that



Hussain is the first hacker to be explicitly targeted by the US in a military campaign. (The 2011 killing of Anwar al-Awlaki in Yemen via a September 2011 drone strike offers an example of prior military action to end recruiting via the Internet.)

And beyond the Hussain strike, the US has initiated a ‘doxing’ prosecution, that of Ardit Ferizi, a Kosovar studying computer science in Malaysia. Arrested in October 2015, Ferizi allegedly breached a retailer’s database and lifted records of all its military and government customers. US prosecutors allege, “Ardit Ferizi is a terrorist hacker who provided material support to ISIL by stealing the personally identifiable information of US service members and federal employees and providing it to ISIL for use against those employees,” and provided Hussain with this information between June and August 2015. (Department of Justice Office of Public Affairs, 2015)

Since Hussain’s death, ISIL has continued to mount cyber campaigns, however its aspirations appear far greater than its capabilities today. (Marks, ISIL Aims to Launch Cyberattacks on U.S., 2015) Yes, ISIL can hire individuals online to act on the group’s behalf in launching cyber-attacks, but likely only to a limited degree. (Bennett & Viebeck, 2015) ISIL cyber operatives continue advancing technologically as they learn to shield their communications from eavesdropping, utilizing encrypted chat systems and employing faked phone numbers. Although, these cyber-attacks are low in threat capability and are able to be stopped, ISIL is beginning to learn and hone their skills as they make headlines in 2016 for their exploits in cyberspace. (Lohrmann, 2015) As hackers around the world become more sophisticated, terrorist groups are likely to follow their lead and use the same tools to further their ends. Soon the US may be faced with a major cyber capability in the hands of a Jihadist group[s].

## Policy Options – Cyber Offense Against ISIL

Although ISIL's military capabilities in Iraq have been significantly blunted and to a lesser degree Syria, the organization remains a force in being. The challenge in further reducing ISIL's cyber capabilities is twofold. Work must be done to further harden military, critical infrastructure and economic targets. Mitigating the ISIL social media machine is a difficult but necessary task. There is no silver bullet available to resolve the power of pro-ISIL narratives especially as Muslims living in the West face hostility and even persecution. (Callimachi, ISIS and the Lonely Young American, 2015) As spectacular terror attacks generate considerable fear among the electorates in the West, ISIL's use of cyber tactics for intelligence collection, recruitment, and kinetic attack may be met with louder calls for intensive Internet monitoring to support the counter terror mission.

Translating desired policies into real, viable cyber options is the unique challenge of the moment. In June 2016, a dissent memorandum signed by 51 US State Department diplomats argued for a more rigorous effort to bring about a cessation of hostilities in Syria. While the diplomats argued for, "a more militarily assertive US role in Syria," they prefer to leverage kinetic technologies such as precision-guided weapons and air defense systems for offensive and defensive roles, respectively. (The New York Times, 2016) The memo stressed a policy where belligerence by any of the unpopular warring parties (e.g. the Syrian regime and ISIL) would be met with force. The question in need of considering as well is how cyber forces could be employed to further degrade ISIL's ability to wage war as well as forcing the Assad government to acquiesce to a holding ceasefire.

As the top Pentagon leadership has mentioned cyber “bombs” that it wishes to deploy, the issue for the organization is to begin considering what sort of cyber munitions, capabilities, or tactics might make the most headway in reducing ISIL’s battlefield capabilities. What then must take place is a mapping of desired capabilities to an assessment of what is technically feasible now or with varying degrees of effort. There are likely three desired cyber combatant areas in which most activity should fall: intelligence gathering from cyberspace’s fixed and mobile computational infrastructure including networks both wired and wireless; cyber-attack capabilities designed to degrade or damage battlefield effectiveness of targeted forces; and cyber-information campaigns against enemy messaging.

While it is impossible to know much of the current cyber-signals intelligence capabilities held by the US without moving into the classified space, we can conjecture on the sorts of capabilities that may be desirable in sweeping up additional intelligence resources. One of the items leaked by Edward Snowden was Tailored Access Operations (TAO), the capacity to gain entry to important systems by either physical or virtual means. What would be enormously useful is to have the capacity for TAO at a distance. Operational units would call upon lightweight technologies to pull intelligence, map digital points of presence, and see (in real time) data linkages on the battlefield and beyond it. Holding measurement and signatures mapping of the computer terrain might bring useful capabilities in intelligence collection and targeting as well.

While ISIL’s combatants are wedded to the same armaments seen in civil conflict from the Vietnam and Angola to Somalia and Bosnia, chiefly the Kalashnikov rifle and the rocket-propelled grenade, the lure of adopting more sophisticated weaponry will likely grow. As the Internet of Things (IoT) extends to vehicles and other tools employed by ISIL and other insurgents, the potential will grow for cyber-attack against them. While hackers at the DEFCON and Black Hat

conferences have made news with car hacking, CyberCom probably should begin thinking about how to get inside the computing components of the Toyota Hilux and Land Cruiser 4x4 vehicles that are key to the mobility of Jihadist elements from Mogadishu to the Maghreb. (Rosenblatt, 2013) Today, ISIL is using drones and for this reason, CyberCom should be putting resources into monitoring or disabling their control systems whether in defensive postures around key installations such as nuclear power stations or government buildings or on the offensive, denying ISIL and its successors the drone intelligence and transport capability on the battlefield. These may be non-lethal attacks, and that would be of utility in minimizing collateral casualties and reducing insurgent capabilities. We should accept a point from Harvey Sapolsky on non-lethal cyber capabilities who told a reporter regarding non-lethal ammunition, “The first time a Marine shoots a bad guy with a beanbag, and the bad guy gets up and shoots back, will also be the last time the Marine uses the beanbag.” Nonetheless, there will be no shortage of kinetic hacking targets for the Defense Department.

Also, seemingly infinite are the messages conveyed by the Internet to support ISIL’s war effort. While the platforms – such as Twitter, Instagram, and YouTube – used to convey Jihadist messaging can police their content to a degree, the US government straddles a fine line in censoring ISIL and others like it in cyberspace. The IC will no doubt continue its work in seeing the full contents of social media outlets in a manner not dissimilar from how the Middle Eastern governments overthrown by the Arab Spring sought to do so. The key for short-circuiting communications for ISIL may be to borrow the concept of ransomware, the encryption of key data on important systems that has mushroomed in cybercrime. Encrypting stored data or even data in transit that is threatening to the fight against ISIL and its recruitment efforts may be a useful tool.

So too might be technical failures of commodity computing hardware triggered by cyber-attack. Think of such tools as Stuxnet for data obfuscation or deletion.

What will be important for their three general areas is to adopt a culture of innovation that is inclusionary of heterogeneous ideas and actors. The IC has employed its startup venture capital vehicle, In-Q-Tel, to develop desired capabilities where the commercial technology industry has not seen opportunity. As the Cold Warriors employed aerospace skunk works to develop world changing technologies like the U-2, SR-71, and F-117, the cyber warriors will need to create a capability at the intersection of Silicon Valley and the Pentagon that delivers innovative, unorthodox cyber tools and weapons that may move from idea to deployment on a schedule far faster than the norm for the government. This would likely take form in a linkage between CyberCom's geeks and SOCOM's (US Special Forces Command) operators. Much as the special operations community in the US military has built unique transport, intelligence, and support capabilities around itself, it will need a cyber echelon housed within its intelligence component as well. Already arguments have begun to emerge for a "Cyber JSOC" (Joint Special Operations Command), the analog to SOCOM's JSOC force composed of Army Delta and Navy DEVGRU (Special Warfare Development Group) direct action units as well as its Intelligence Support Activity. (CyberWar.News, 2016)

There will no doubt be difficulties in incorporating cyber operations components into overall US strategy on countering ISIL and other non-state foes, however, it is fairly clear that the top national security leadership in Washington wants to leverage cyber capabilities more significantly. One issue that will continue to dog offensive cyber operations and intelligence activities is that of the equities question – that is to what degree the US government should turn over knowledge it accrues regarding cyber vulnerabilities to the technology industry so that they

may be repaired. For instance, is it more desirable for the CyberCom and the NSA to hold onto information regarding broken encryption implementations or software as was alleged regarding the Heartbleed bug in the OpenSSL software libraries. Issues such as this will be an important question for policy.

Ultimately, the cyber conflict against ISIL will serve as a template for future cyber action against terror groups, insurgents, and violent transnational criminal syndicates. Looking backward, we can see just how effective the application of robust signals intelligence capabilities have been. Consider US support of Colombian operations against the Fuerzas Armadas Revolucionarias de Colombia (FARC). There can be little doubt that the Colombian military and police were made significantly more effective with the addition of bespoke US intelligence capabilities. Policymakers are keen to eradicate or at least damage ISIL, a group without state sponsorship. They will need to ask how cyber weapons can frustrate it as much as anything else. The more cyber tactics can short-circuit ISIL's operational capabilities, the better. What is necessary for the cyber operators are clear objectives from senior leadership on what they want to produce. The engineers that build CyberCom's tools and the hackers that serve as its operational forces can easily enough push back on what they believe not to be possible.

## Glossary of Abbreviations

APT – Advanced Persistent Threat

CyberCom – Cyber Command

DEVGRU – United States Naval Special Warfare Development Group (SEAL Team Six)

DNC – Democratic National Committee

FARC – Fuerzas Armadas Revolucionarias de Colombia

IC – Intelligence Community

ICIJ – International Consortium of Investigative Journalists

IoT – Internet of Things

ISIL – Islamic State in Iraq and the Levant

ISIS – Islamic Stat in Syria

ISR – Intelligence, Surveillance, and Reconnaissance

JSOC – Joint Special Operations Command

NSA – National Security Agency

SOCOM – United States Special Operations Command

SOF – Special Operations Forces

TAO – Tailored Access Operations

US – United States

UK – United Kingdom



## References

- Alexander, H. (2016, February 4). *Why is Julian Assange still inside the embassy of Ecuador?* Retrieved from The Telegraph.
- Almasy, S. (2015, June 4). *Boston Shooting: Who Was Usaamah Rahim?* Retrieved from CNN U.S.
- Applegate, S. D. (2013). *The Dawn of Kinetic Cyber. 2013 5th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications.
- Becker, O. (2014, July 12). *ISIS Has a Really Slick and Sophisticated Media Department*. Retrieved from VICE News.
- Beene, K. (2016, May 4). *Who are the cyberwar superpowers?* Retrieved from World Economic Forum.
- Bennett, C., & Viebeck, E. (2015, May 17). *ISIS Preps for Cyber War*. Retrieved from The Hill.
- Birchall, C. (2014, February). *Radical Transparency?* Retrieved from Cultural Studies: Critical Methodologies.
- Blanchette, D. (2016, March 20). *Homeland Security Expert: ISIS Thrives on Social Media*. Retrieved from The State Journal-Register.
- Brenner, J. (2013). *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World*. New York: Penguin.
- Bronk, C. (2016). *Cyber Threat: The Rise of Information Geopolitics in U.S. National Security*. Retrieved from Praeger: Santa Barbara.

Callimachi, R. (2015, June 27). *ISIS and the Lonely Young American*. Retrieved from The New York Times.

Callimachi, R. (2015, June 27). *ISIS and the Lonely Young American*. Retrieved from The New York Times.

CBS DC. (2014, June 17). *ISIS Launches Twitter App For Android Phones*. Retrieved from CBS DC.

CBS News. (2014, August 29). *ISIS Recruits Fighters through Powerful Online Campaign*. Retrieved from CBS News.

Chen, A. (2015, June 2). *The Agenc*. Retrieved from The New York Times.

Chivers, C. J. (2016, April 6). *Facebook Groups Act as Weapons Bazaars for Militias*. Retrieved from The New York Times.

Coleman, G. (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Brooklyn: Verso.

Cuthbertson, A. (2014, June 18). *Iraq Crisis: Isis Launch Twitter App to Recruit, Radicalise and Raise Funds*. Retrieved from International Business Times.

CyberWar.News. (2016, April 27). *U.S. Needs 'Cyber JSOC' So It Can Strike Harder, Faster In Event Of Conflict: Experts*. Retrieved from CyberWar.News.

Dabashi, H. (2016, July 5). *ISIL turns 'shock and awe' doctrine against Islam*. Retrieved from Al Jazeera.

Deibert, R. (2015, January). *The Geopolitics of Cyberspace After Snowden*. Retrieved from Current History.

Department of Justice Office of Public Affairs. (2015, October 15). *ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges*. Retrieved from Department of Justice Office of Public Affairs.

Eisenstadt, M. (2014, November 3). Defeating ISIS: A Strategy for a Resilient Adversary and an Intractable Conflict. *Policy Notes – The Washington Institute for Near East Policy*(20).

FireEye. (2016). *Redline Drawn: China Recalculates its Use of Cyber Espionage*. Milpitis: FireEye.

Fisher, M. (2016, July 26). *Why Security Experts Think Russia Was Behind the D.N.C. Breach*. Retrieved from The New York Times.

Francecshi-Bicchierai, L. (2015, August 28). *How a Teenage Hacker Became the Target of a US Drone Strike*. Retrieved from Motherboard.

Garber, M. (2014, March 6). *Doxing: An Etymology*. Retrieved from The Atlantic.

Goldman, D. (2016, February 5). *Twitter goes to war against ISIS*. Retrieved from CNN Money.

Goldman, D. (2016, February 5). *Twitter Goes to War against ISIS*. Retrieved from CNN Money.

Gonzalez, E. (2015, September 5). *Kurdish Peshmerga: Divided from Within*. Retrieved from Harvard Political Review.

Grove, T., & Kesling, B. (2016, April 21). *Russia Pursues Ties With Kurds to Keep Foothold in Region*. Retrieved from Wall Street Journal.

Guynn, J. (2016, January 30). *Facebook Bans Private Gun Sales*. Retrieved from USA Today.

Hall, J. (2015, April 10). *European ISIS Fighters Who Are Seen as Cannon Fodder by Their Commanders Desperately Try to Prove Their worth by Committing the Most Sickening Atrocities, Says Former Prisoner*. Retrieved from Mail Online.

Haq, H. (2014, 22 October). *ISIS Excels at Recruiting American Teens: Here Are Four Reasons Why (+Video)*. Retrieved from The Christian Science Monitor.

Heickerö, R. (2010). *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. Stockholm: Swedish Defence Research Agency.

Hubbard, B., & Sheikh, M. (2015, July 16). *WikiLeaks Shows a Saudi Obsession With Iran*. Retrieved from The New York Times.

Kaspersky Lab. (2015). *Equation Group: The Crown Creator of Cyber-Espionage*. Kaspersky Lab.

Kelly, B. B. (2012). Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cyber Security Reform. *Boston University Law Review*, 92(4).

Lee, D. (2014, August 21). *Diaspora Social Network Cannot Stop IS Posts*. Retrieved from BBC News.

Lohrmann, D. (2015, May 18). *Cyber Terrorism: How Dangerous Is the ISIS Cyber Caliphate Threat?* Retrieved from Government Technology.

MacAskill, E., & Dance, G. (2013, November 1). *NSA Files: Decoded*. Retrieved from The Guardian.

- Mandiant. (2013). *APT1: Exposing One of China's Cyber Espionage Units*. Mandiant.
- Marks, J. (2015, December 29). *ISIL Aims to Launch Cyberattacks on U.S.* Retrieved from Politico.
- Marks, J. (2015, December 29). *ISIL Aims to Launch Cyberattacks on U.S.* Retrieved from Politico.
- Mchugh, J. (2015, December 29). *ISIS Cyber Attack? US Government, Planes Threatened With Malware, Hacking By Islamic State*. Retrieved from International Business Times.
- Moore, J. (2015, 4 December). *Why air strikes alone can't destroy ISIS*. Retrieved from Newsweek.
- Murphy, L. (2015, December 15). *The Curious Case of the Jihadist Who Started Out as a Hactivist*. Retrieved from Vanity Fair Hive.
- Nader, A. (2015). *Iran's Role in Iraq*. Retrieved from RAND: Santa Monica.
- Olson, P. (2013). *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York: Back Bay Books. Retrieved from Back Bay Books: New York.
- Paganini, P. (2015, October 26). *Mikko Hyppönen Warns the ISIS Has a Credible Offensive Cyber Capability*. Retrieved from Security Affairs.
- Pagliery, J. (2014, July 2). *Russia Attacks U.S. Oil and Gas Companies in Massive Hack*. Retrieved from CNN Money.

- Pagliery, J. (2015, October 16). *ISIS Is Attacking the U.S. Energy Grid (and Failing)*. Retrieved from CNN Money.
- Rosenblatt, S. (2013, August 2). *Car hacking code released at Defcon*. Retrieved from CNET Security.
- Sanchez, R. (2015, June 5). *ISIS Exploits Social Media to Make Inroads in U.S.* Retrieved from CNN U.S.
- Segal, A. (2016, June 27). *Cyber Conflict After Stuxnet*. Retrieved from Council on Foreign Relations.
- Shamah, D. (2014, 17 December). *Devastating Sony hack just a malware rehash, say experts*. Retrieved from The Times of Israel.
- Singer, P., & Brooking, E. (2015, December 11). *Terror On Twitter: How ISIS Is Taking War to Social Media - And Social Media Is Fighting Back*. Retrieved from Popular Science.
- Stavridis, J. (2013, June 20). *The New Triad*. Retrieved from Foreign Policy.
- Taylor, A. (2014, March 21). *Why Turkey banned Twitter (and why banning Twitter isn't working)*. Retrieved from Washington Post.
- The Atlantic. (2014, June). *How ISIS Games Twitter*. Retrieved from The Atlantic.
- The Guardian. (2016, May 22). *Isis Leader Encourages Lone Wolf Attacks on Civilians in Europe and US*. Retrieved from The Guardian.
- The New York Times. (2016, June 17). *State Department Draft Dissent Memo on Syria*. Retrieved from The New York Times.

Trianni, F., & Katz, A. (2014, September 5). *Why Westerners Are Fighting for ISIS*. Retrieved from Time.

Waterman, S. (2007, June 11). *Analysis: Who cyber smacked Estonia?* Retrieved from UPI.

Webb, S. (2015, May 15). *ISIS Use Instagram to Post Sickening Bodycam Footage of Murderous Assault on Civilians in Iraqi City*. Retrieved from Mirror.

Yan, H. (2014, September 4). *Showing off its crimes: How ISIS flaunts its brutality as propaganda*. Retrieved from CNN Regions.

Zero Censorship. (2016, February 3). *ISIS Beheading Four Prisoners*. Retrieved from Zero Censorship.

Zetter, K. (2015, November 19). *Security Manual Reveals the OPSEC Advice ISIS Gives Recruits*. Retrieved from Wired.

THIS PAGE  
INTENTIONALLY  
LEFT BLANK





# Resiliency in Operational Technology

## Table of Contents

Table of Figures .....	2
Introduction.....	3
Critical Infrastructure.....	4
The Interdependencies of Critical Infrastructure .....	6
Operational Technology.....	8
Industrial Control Systems and its Subsets.....	9
Purdue Model for Control Hierarchy .....	11
Operational Technology VS Information Technology .....	14
Security Implications Caused by OT/IT Convergence .....	16
Resiliency.....	20
Modified Purdue Model for Control Hierarchy .....	21
Location, Location, Location.....	26
Characteristics of a Resilient System.....	28
Prerequisites of a Resilient System.....	31
Conclusion .....	33
Glossary of Abbreviations .....	34
References.....	36

## Table of Figures

Figure 1: US Critical Infrastructure Sectors with EPCIP Counterparts Marked with Orange .....	5
Figure 2: Examples of CI Interdependencies (Phillips, 2009).....	7
Figure 3: Comparison of SCADA and DCS (Kumar, 2017) .....	9
Figure 4: Purdue Model for Control Hierarchy (Conklin, 2016).....	11
Figure 5: OT Architecture Baseline (Obregon, 2015) .....	14
Figure 6: OT VS IT (Shinder, 2001).....	15
Figure 7: October 21, 2016 Internet Outage Heat Map (Krebs, 2016) .....	18
Figure 8: Modified Purdue Model for Control Hierarchy .....	21
Figure 9: Communication Channels without Resiliency .....	23
Figure 10: Communication Channels with Resiliency .....	23
Figure 11: Modified ICS Network Diagram (Byres, 2011).....	27
Figure 12: Example of Terms Typically Used for Resiliency .....	28
Figure 13: Characteristics Overlap .....	30
Figure 14: Good, Better, Best of Resilience .....	30

# Introduction

In February of 2013, President Barack Obama issued *Presidential Policy Directive 21* (PPD-21) which revolves around the subject of ‘critical infrastructure security and resilience’. This directive attempts to unify and advance a nationwide effort to “strengthen and maintain secure, functioning, and resilient critical infrastructure”. (The White House Office of the Press Secretary, 2013) The term ‘resilience’, according to the PPD-21, means “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions”. It also includes “the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents”. These definitions feel lacking in depth. The PPD-21 falls short of truly explaining what resiliency is and how it applies to critical infrastructure.

There are essentially two major sections in this paper, with numerous subsections. The first section elaborates on what critical infrastructure is and why it is significant. This section also includes a high-level overview of how operational technology (OT) relates to CI, and also illustrates the differences between OT and information technology (IT). This section then finishes with an overview of some of the information security (IS) concerns related to the convergence of OT and IT.

The second section of this paper elaborates on what resiliency is and how it compliments OT. The Purdue Model for Control Hierarchy is modified to incorporate a new resiliency layer, which aids in the design of a resilient system. The next section details the varying characteristics a resilient system will exhibit. And finally, this section includes a review of some of the prerequisite work that needs to be completed in order to design a resilient system.

### Critical Infrastructure

Modern societies are highly dependent on the continuous operation of CI. (European Union Institute for Security Studies, 2016) CI refers to the essential services that underpin society and serve as the backbone of a nation's assets "in which their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof". (Department of Homeland Security, 2016) In other words, the power, water, transportation, grocery stores, and communications we utilize every day are all significant to the security and safety of our society. This shows the importance of CI, and the need to decrease the chances of disruption to society by protecting and making CI resilient to internal or external abnormalities. An abnormality in this paper refers to any event that could potential hurt the performance of a system or process. Weather disasters, terrorist attacks, insider threats, unintentional employee mistakes are just a few examples of an abnormality.

Every country in the world has CI. Although developed countries like the United States (US) typically have more technological prowess and financial capability than other countries, most of the CI around the world is similar in design. The US has designated 16 sectors pertaining to the CI of the nation, while the European Programme for Critical Infrastructure Protection (EPCIP) on the other hand has identified 11 CI Sectors for the European Union (EU) and the European Economic Area (EEA). (European Commission, 2006) The figure below illustrates the US's 16 CI sectors with the EPCIP's counterparts denoted by an orange box. (Department of Homeland Security, 2016) EPCIP also lists Space and Research Facilities in their CI sectors, these are omitted from denotation in the list below since there is no directly related sector in the US, as these two sectors are incorporated into other US CI sectors.

Chemical	Commercial	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	Water and Wastewater Systems

*Figure 1: US Critical Infrastructure Sectors with EPCIP Counterparts Marked with Orange*

### The Interdependencies of Critical Infrastructure

Although CI is separated into distinct sectors, the physical and logical design of CI systems is much more blurred. It is common for CIs to be connected through a wide variety of mechanisms at multiple points. These connections, to oversimplify the view of CI overall, look like a “system of systems”. (Rinaldi, Peerenboom, & Kelly, 2001) These connections between CI’s are what Rinaldi, Peerenboom, & Kelly refer to as interdependencies. According to them, interdependency is the “bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other (i.e. two infrastructures are interdependent when each is dependent on the other). When anomalies happen, these interdependencies can cause quickly cascading disruptions into multiple CI sectors, causing havoc at various degrees depending on the strength of the relationships.

For an example of an interdependency, let's take a natural gas pipeline that is supplying fuel to a power plant. The pipeline provides the fuel for the power plant, while the power plant generates the electricity necessary to run the various components of the pipeline itself, this is a basic interdependency. If a hurricane destroys part of the pipeline, the power plant will not have the fuel necessary to generate power. This will have cascading effects in other CIs, such as insufficient power to run communication networks properly, which will slow emergency services down, and so on and so forth. The figure below illustrates other examples of CI interdependencies. (Phillips, 2009)

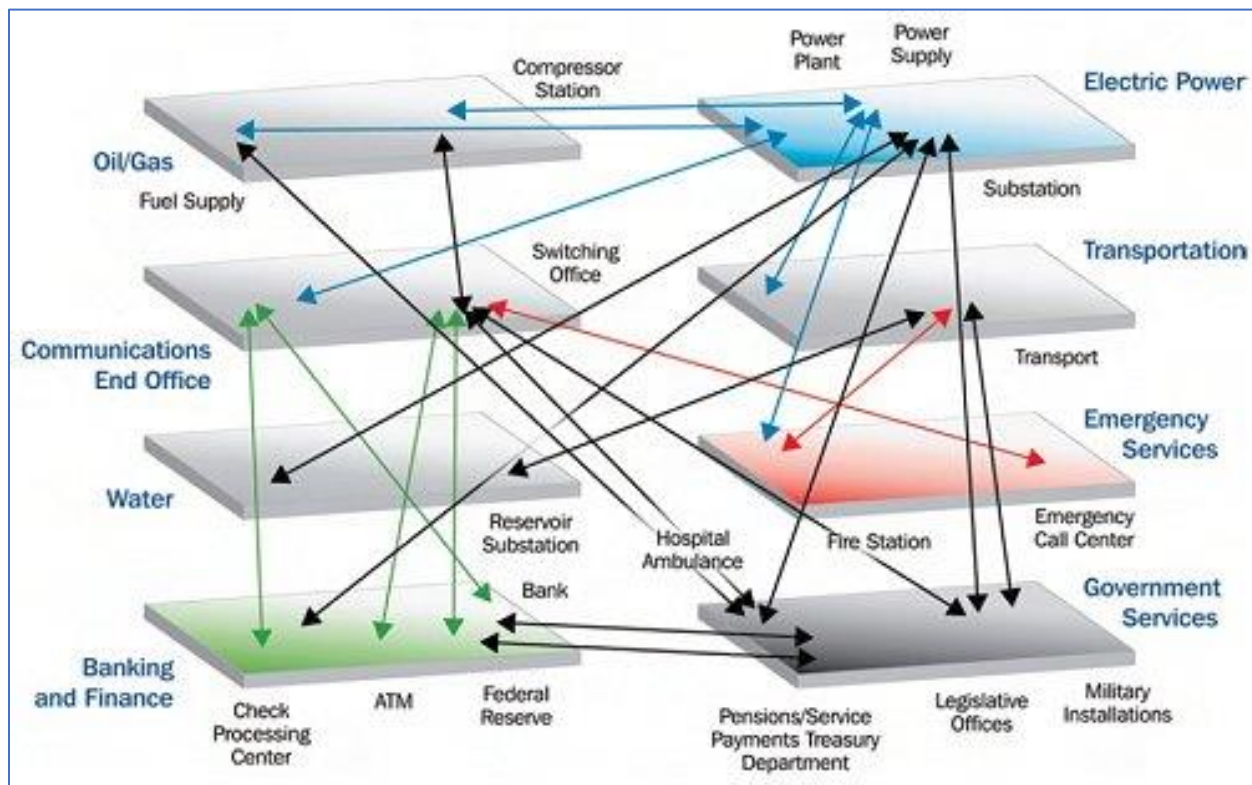


Figure 2: Examples of CI Interdependencies (Phillips, 2009)

Understanding these interdependencies between CIs is no simple task and can complicate and prolong the model generation and analysis process very quickly. But it is necessary to understand the interdependencies of, for example a nuclear power plant, so that one will be able



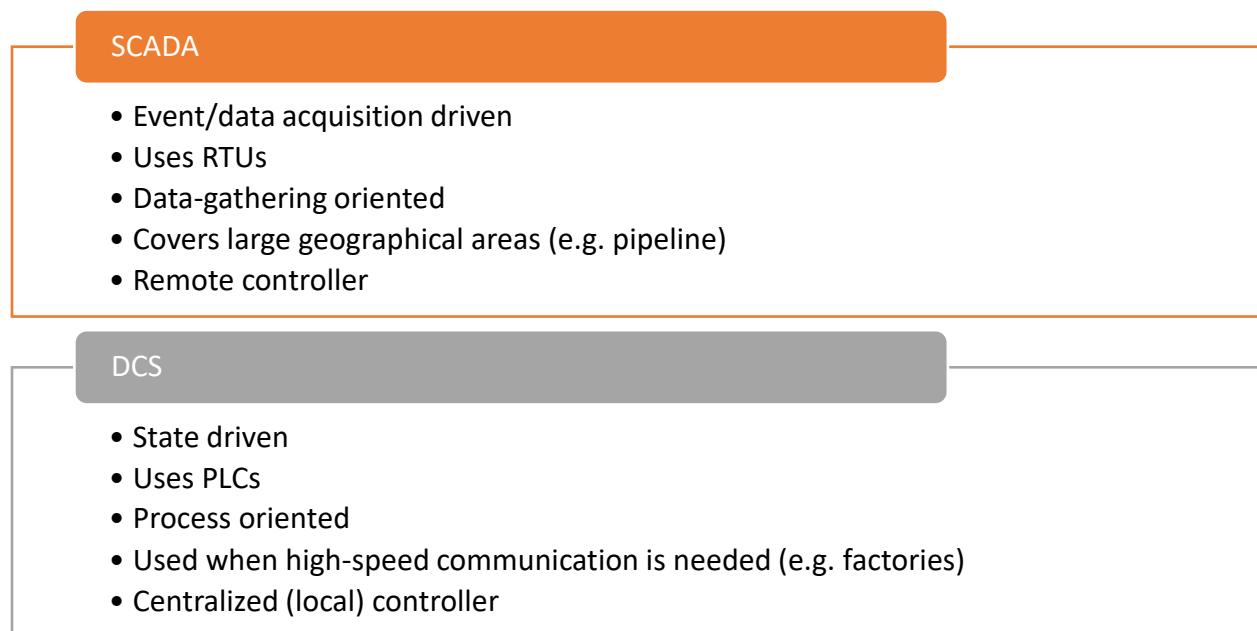
to understand potential external threats to the plant. This same external interdependency analysis can be conducted on internal systems as well. This identification of external and internal interdependencies is a step in the process of gathering data for a resilient system design. Ignoring the interdependencies, will show only a partial viewpoint, and will prevent a holistic approach to making a system resilient.

## Operational Technology

OT is the general term used to refer to the overall design and implementation of hardware, software, and concepts that allow the Industrial Controls Systems (ICS) of CI to function. (Wikipedia, 2017) It includes all layers of all systems within a CI. (Beal, n.d.) OT is not exclusive to the sophisticated world of CI though, as it can be found in many locations. Ships, airplanes, trains, cars, traffic systems, refineries, waste water systems, home and fire sprinkler systems, factories, the charging process for cell phones, car manufacturing plants, and various medical equipment is just a tiny portion of where OT is located. (Conklin, 2016) Even though OT is synonymous with ICS, OT is the term typically used when referring to the interconnectivity of ICS network to an IT network, this also known as IT/OT convergence. (Rouse & Haughn, 2016) One example of IT/OT convergence is when a manufacturing plant connects its ICS network to that of the IT network on the corporate side. Another example is Internet of Things (IoT) devices. OT, ICS, and SCADA are often referred to synonymously on media outlets today, but in all reality, there are differences (sometimes subtle) between their definitions and what they represent.

### Industrial Control Systems and its Subsets

ICS refers to a device or a set of devices that manage, command, direct, and/or regulate the behavior of other devices systems. (Conklin, 2016) In other words, ICS is comprised of systems that are used to control and monitor industrial processes. (Williamson, 2015) Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Building Automation Systems (BAS), and Smart Grid systems are just a few of the subsets of ICS. (Byres, SCADA Security Basics: SCADA vs. ICS Terminology, 2012) Differences between SCADA and DCS are illustrated in the figure below. (Kumar, 2017)



*Figure 3: Comparison of SCADA and DCS (Kumar, 2017)*

These differences between SCADA and DCS were more distinguished earlier on in time. As time has progressed though, the lines are becoming more blurred as SCADA manufacturers have started to incorporate more DCS functionality. While DCS manufacturers have lowered response timing closer to that of a SCADA system. (Wavestone, 2015)

BAS refers to a DCS that controls and monitors the security, mechanical, fire, lighting, safety, and HVAC systems of a building. (Control Services, n.d.) BAS is also known as a “smart building” or “smart home” depending on the application of BAS. This automation system ensures operational performance of the building, as well as the comfort and safety of the occupants of the building. (KMC Controls Inc., 2013)

## Purdue Model for Control Hierarchy

The Purdue Model for Control Hierarchy is the *de facto* standard model that divides Enterprise and OT networks into segments comprised of systems that have similar design and/or requirements. (Obregon, 2015) This model consists of 5 zones and 5 subsequent levels. Figure 4 shows the zones and levels of this model. (Conklin, 2016) Each zone and level are subsequently described after the figure.

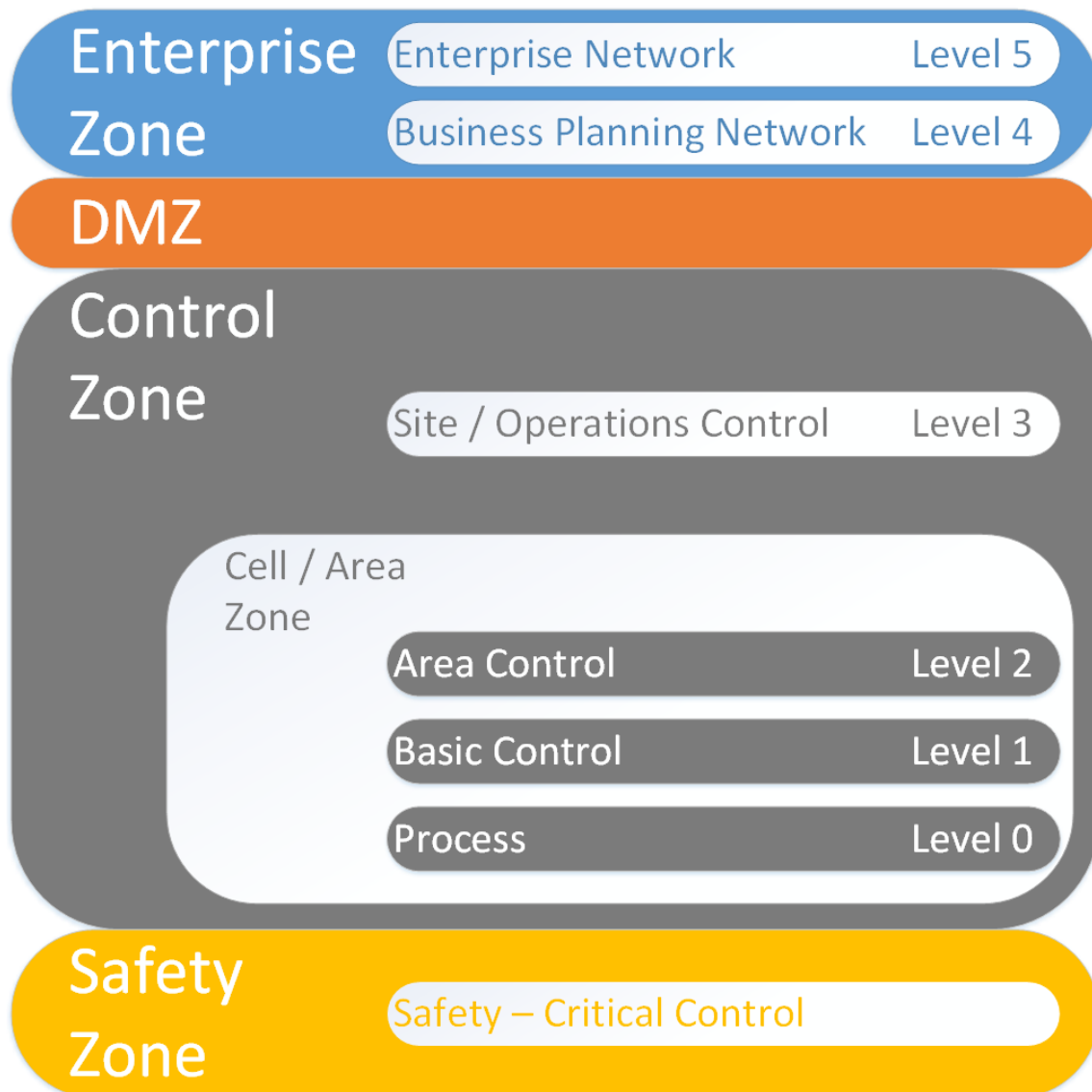


Figure 4: Purdue Model for Control Hierarchy (Conklin, 2016)

- **Enterprise Zone:** Typically managed by IT admins of the organization.
  - **Level 5: Enterprise Network** – Corporate IT infrastructure systems and applications (e.g. Virtual Private Network (VPN) and Internet Access). (Chandra, 2015)
  - **Level 4: Business Planning Network** – Corporate IT systems responsible for e-mail, reporting, phone and printing services, scheduling, and similar applications. (Obregon, 2015)
- **DMZ:** (Demilitarized Zone) Segmented buffer area where data can be shared between the Enterprise and Control zones; usually between two differently configured firewalls (or equivalent). (Chandra, 2015)
- **Control Zone:** (aka Manufacturing Zone) Consists of all the activities within Levels 0 through 3. Typically maintained by the OT admins of the organization.
  - **Level 3: Site / Operations Control** – Services, applications, and systems responsible for managing control operations that produce the end product (e.g. historian, staging area, network management, and production scheduling). (Obregon, 2015) Systems in Level 3 typically communicate with Levels 0 and 1, and Levels 4 and 5 through the DMZ.
- **Cell / Area Zone:** Functional area of a manufacturing facility. It is not unusual for many Cell / Area Zones to exist in a Control Zone. (Cisco, 2013)
  - **Level 2: Area Control** – Manufacturing operations for a single production cell / area (e.g. Human Machine Interface (HMI), control room workstations, and supervisory control). (Obregon, 2015) Level 2 typically communicates with Level 1.

- **Level 1: Basic Control** – Consists of controllers with the primary function of interfacing with Level 0 devices, as to manipulate or direct the manufacturing process. (Cisco, 2013) An example of a controller is a Programmable Logic Controller (PLC) or a Remote Terminal Unit (RTU).
- **Level 0: Process** – Consists of the sensors, actuators and instrumentation elements that are directly connected to the manufacturing process. (Cisco, 2013) This includes functions as simple as opening and closing a valve to more complex functions, such as a robotic arm moving to weld car frame pieces together.
- **Safety Zone:** Safety is considered the highest priority in the OT space. This zone consists of the systems and components that monitor the manufacturing process for any anomalies that exceed a defined threshold. These systems are also responsible for alerting operators of any unsafe conditions and trigger the necessary safety precautions deemed necessary by the safety system, which can include shutting down operations in the safest way possible. (Obregon, 2015) Safety systems should be separate from the other manufacturing networks in place, but this is not always the case in the real-world applications.

The Purdue Model for Control Hierarchy, first developed by the International Society of Automation ISA-99 Committee for Manufacturing and Control Systems Security, forms the design baseline for an OT architecture, shown in Figure 5 below. (Obregon, 2015)

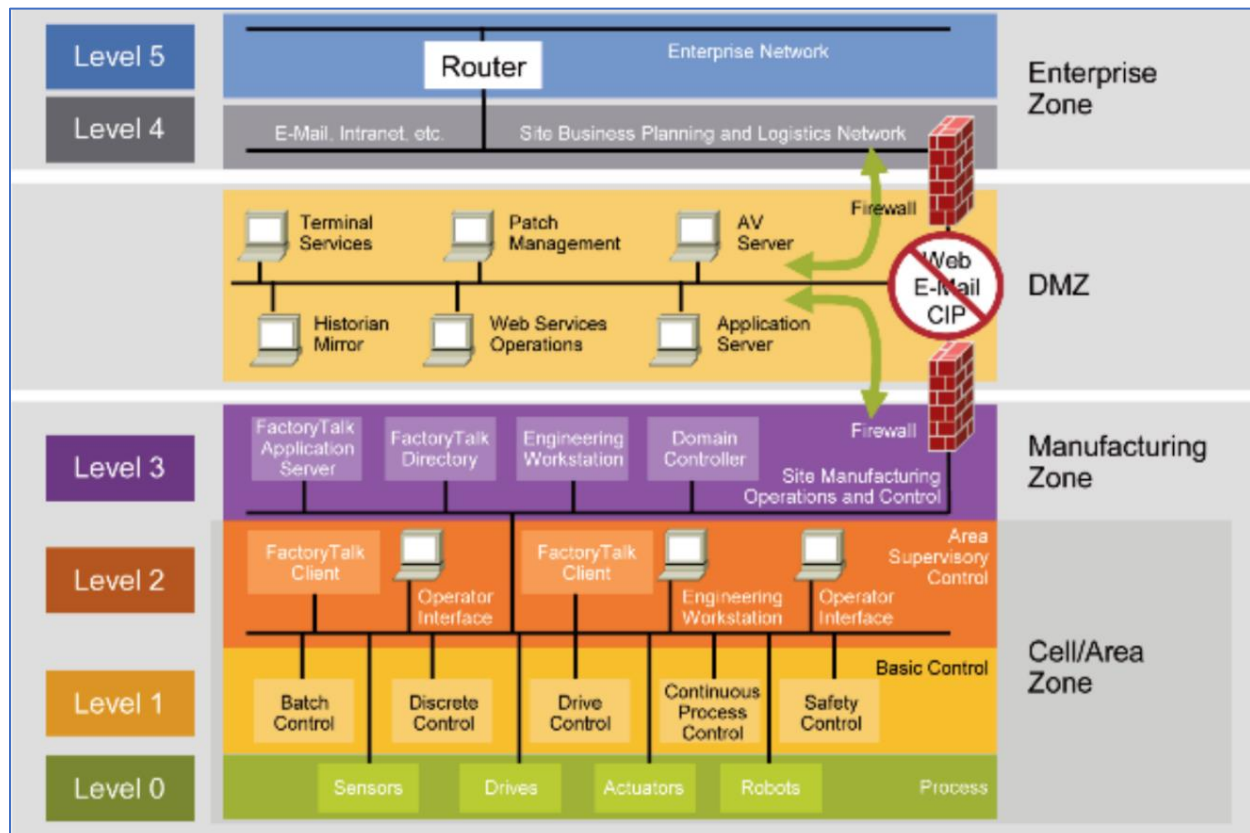
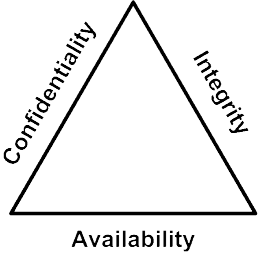


Figure 5: OT Architecture Baseline (Obregon, 2015)

## Operational Technology VS Information Technology

As mentioned earlier, OT is vastly different than IT. OT handles the interfacing related to data with the physical world, while IT handles data. The primary concern of OT is the continued safe operation of the system. A common misconception is that IT principles and design apply directly to OT. This is not the case, especially for IS related items. As IT systems are typically replaced or upgraded every 3 – 5 years, OT components need to last around 25 years (even longer in some cases). Most people do not even own houses that old. Even with penetration testing (a

major component of IS) running an intense Nmap scan (nmap -T4 -A -v) can cripple ICS components, such as PLCs and prevent them from operating, even brick them. There are also numerous other differences that are illustrated in *Figure 6: OT VS IT*, located below. (Shinder, 2001)

<b>Operational Technology</b>		<b>Information Technology</b>
My system was working yesterday, my system is working as expected today, if nothing happens it should continue tomorrow.		
20 years +	<b>Replace/Upgrade Turnover</b>	3-5 years
Continued <b>SAFE</b> operation	<b>Mission</b>	Everything should connect to everything
24/7/365, non-negotiable	<b>Availability</b>	Disruption expected, okay to “unplug” during security incident
Possible loss of property, environment, and/or life	<b>Security Failure Impact</b>	Loss of Personally Identifiable Information (PII)
Numerous vendor-specific protocols, with little or no security built in	<b>Protocols</b>	Standard protocols, with security built in to newer versions
Rarely, if ever	<b>Patching</b>	Applied frequently

*Figure 6: OT VS IT (Shinder, 2001)*



Another major difference between OT and IT is the way hacking takes place. Typically, hacking in the IT space boils down to getting a device to act in such a way or do something it was not truly designed for, usually by gaining escalated privileges, such as administrative rights of a system. But OT systems do not have these privileged and unprivileged credentials below Level 2 (Area Control). Level 1 and Level 0 devices are simple machines in comparison to an IT server. PLCs, for example, follow commands that it receives, nothing more and nothing less. So essentially, the hacker does not need to make a PLC act in a way it was not designed, the hacker just needs to be able to send a simple command (typically the size of a packet), to a PLC to get it to do what they want.

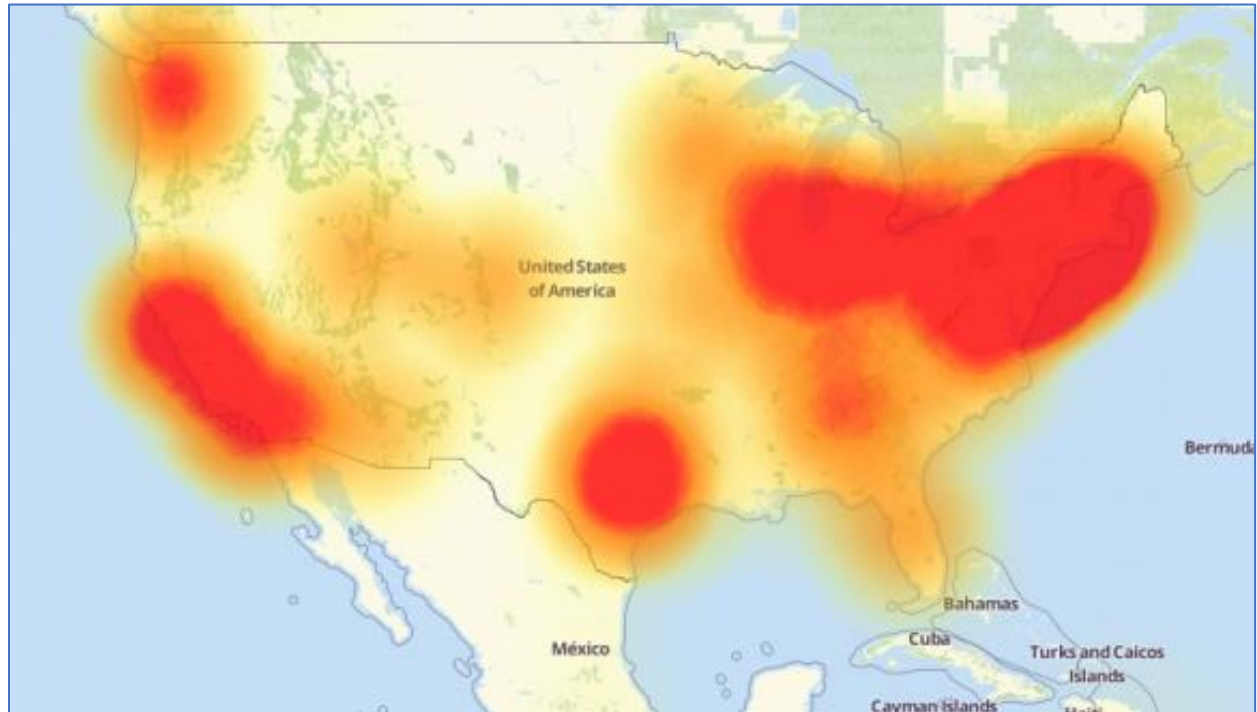
Although the machines running Level 2 and higher resemble more of a PC, the issue here is that these machines are typically older. It is commonplace to see an HMI running Windows XP, which is a very vulnerable operating system (OS). Even if a machine is running a newer OS that supports some security features (such as login credentials), it is common for multiple users to use the same credentials to log into a system, thus defeating the purpose.

### Security Implications Caused by OT/IT Convergence

As technology keeps advancing, more and more OT devices are going to be connected to the internet. As previously stated, OT systems typically have little to no security built into them, which is why connecting them to the internet is such a major security concern. Many organizations are connecting their OT network to the network of the business side as well. This allows for business decisions to be made quickly and decisively. But this comes with a caveat; all the vulnerabilities of the business side network are now a part of the OT network, which creates a larger attack surface for OT systems. More and more OT systems are being hacked for malicious

use, and this can be devastating to the national security of a country. The power grid attack in Ukraine is a prime example of black hat actors actively targeting specific sections of the power grid, causing havoc on the systems, and successfully shutting them down. This operation was an extremely well thought out and planned attack that is unprecedented in the OT space.

Industrial applications are not the only OT/IT convergence, the rise of IoT is contributing as well. IoT shows that consumers want more control of their peripherals through the internet, typically from the ease of a cell phone. These IoT devices typically connect via OT to a central hub, in which the hub itself performs the IT/OT convergence. Other IoT devices connect directly to a Wi-Fi network, these devices also perform IT/OT convergence, just within the device itself, omitting the centralized hub. Because of the growth of the IoT industry, the attack surface of consumer devices has also increased. Many IoT devices that are installed use poor or default passwords. (Palmer, 2016) Some devices from Chinese manufacturers also contain bad or malicious code in their official firmware, that allow backdoor access into a device. (Leyden, 2017) The massive US internet outage that happened in October of 2016 was caused by IoT devices. Hardcoded passwords into the firmware and devices running with default passwords allowed for malware named Mirai to be installed on the IoT device. (Krebs, 2016) In which the attacker was able to create and control a Distributed Denial-of-Service (DDoS) Botnet containing hundreds of thousands of IoT devices. The figure below is a heat map of the internet outage on October 21, 2016 caused by this attack. (Krebs, 2016)



*Figure 7: October 21, 2016 Internet Outage Heat Map (Krebs, 2016)*

These attacks are a good example of why the direct connection of an OT network to an IT network is a poor design. There are solutions to help increase security between the connection of these two networks. Firewalls and data guards are one method, but the best way is to utilize unidirectional gateways. (Conklin, 2016) The benefit of using a unidirectional gateway is that data is never passed into or out of the OT network, only states are passed through. (Waterfall Security, 2016) In other words, when a packet from the IT network contains the command ‘Report Slave ID’, the packet itself is not passed through the gateway. The gateway takes the packet, reads the command, then creates a new packet with the command ‘Report Slave ID’, and sends the newly created packet into the OT network. The original packet that was received is then discarded by the unidirectional gateway.

One might say then, “why don’t we just stick to the old method of air-gapping OT systems”. Well, to quote Stefan Woronka, Siemens Director of Industrial Security Services, “Forget the myth of the air-gap – the control system that is completely isolated is history”. Air-gapping is physically disconnecting a network from any outside connection. While this sounds good in theory, it has proven to be an ineffective way to prevent attacks. (Byres, #1 ICS and SCADA Security Myth: Protection by Air Gap, 2011) Sneakernet still exists despite attempts to truly air-gap a system. Sneakernet is the transfer of data from one computer to another by physical means, such as hard drives, USB flash drives, compact disks, etc. (Wikipedia, 2017) The infection of the Natanz uranium enrichment plant in Iran with the Stuxnet malware is a prime example of the ineffectiveness of air-gapping. (Zetter, An Unprecedented Look at Stuxnet, the World’s First Digital Weapon, 2014)

The Stuxnet and Ukraine power grid attacks do come with a silver lining though. The awareness that this could potentially happen to the US CI has started to grow. It is no longer a theory, it is proven to be possible and very effective. Policy makers within the US are now taking steps to make the CI more secure. PPD-21, as previously stated, is an attempt to nationally unify efforts to “strengthen and maintain secure, functioning, and resilient critical infrastructure.” (The White House Office of the Press Secretary, 2013) One way PPD-21 attempts this is that CI owners and federal agencies are required to cooperatively work together to strengthen resilience and minimize cyber risks. (Vijayan, 2013) ICS black hat hackers are becoming increasingly more knowledgeable of their specific target’s OT systems. More often than not, the adversary has more knowledge of the target than that of the owners of the ICS. (Assante & Lee, 2015) The information sharing should greatly benefit the security of OT system in CI, if it is done properly.

### Resiliency

As previously stated, PPD-21 requires CI operators and federal agencies to work together to make CI OT systems more resilient to attacks. Resiliency will help prevent or minimize the effects of attacks or natural disasters that are inflicted upon an OT system. It will also help prevent cascading effects into other CI sectors through their interdependencies. Resiliency should not be thought of as something just for OT in CI, many other OT systems will benefit from their systems being made more resilient, such as IoT devices or vehicle systems.

But what is resiliency? Resiliency has many different interpretations depending on what discipline to which it is applied. PPD-21 defines resilience “as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions” and includes “the ability to withstand and recover from deliberate attacks, accident, or naturally occurring threats or incidents.” (Department of Homeland Security, 2016) While this is a good definition on paper, it lacks depth. And when one researches further for more depth, various definitions tend to focus solely on the characteristics of a resilient system, which still feels lacking. Another issue is that these various definitions tend to overlap greatly and describe very similar concepts, all while using different terms, in an attempt to distinguish themselves from the rest.

To add more depth to the definition of resiliency, and illustrate where resiliency fits in with OT, a proposed modification to the Purdue Model for Control Systems is made. Then resiliency in OT is further expanded by elaborating on the characteristics and traits a resilient system should demonstrate. Finally, this section ends with some of the prerequisite data collection and modeling that should be completed prior to designing a resilient system.

## Modified Purdue Model for Control Hierarchy

In order to deepen the concept of resiliency for OT, a change to current models is necessary to truly effect change. The change being proposed is the addition of a Resiliency layer (Level .5) to the Purdue Model for Control Hierarchy. It is located in the Control Zone, between Level 1 (Basic Control) and Level 0 (Process). The figure below illustrates this addition.

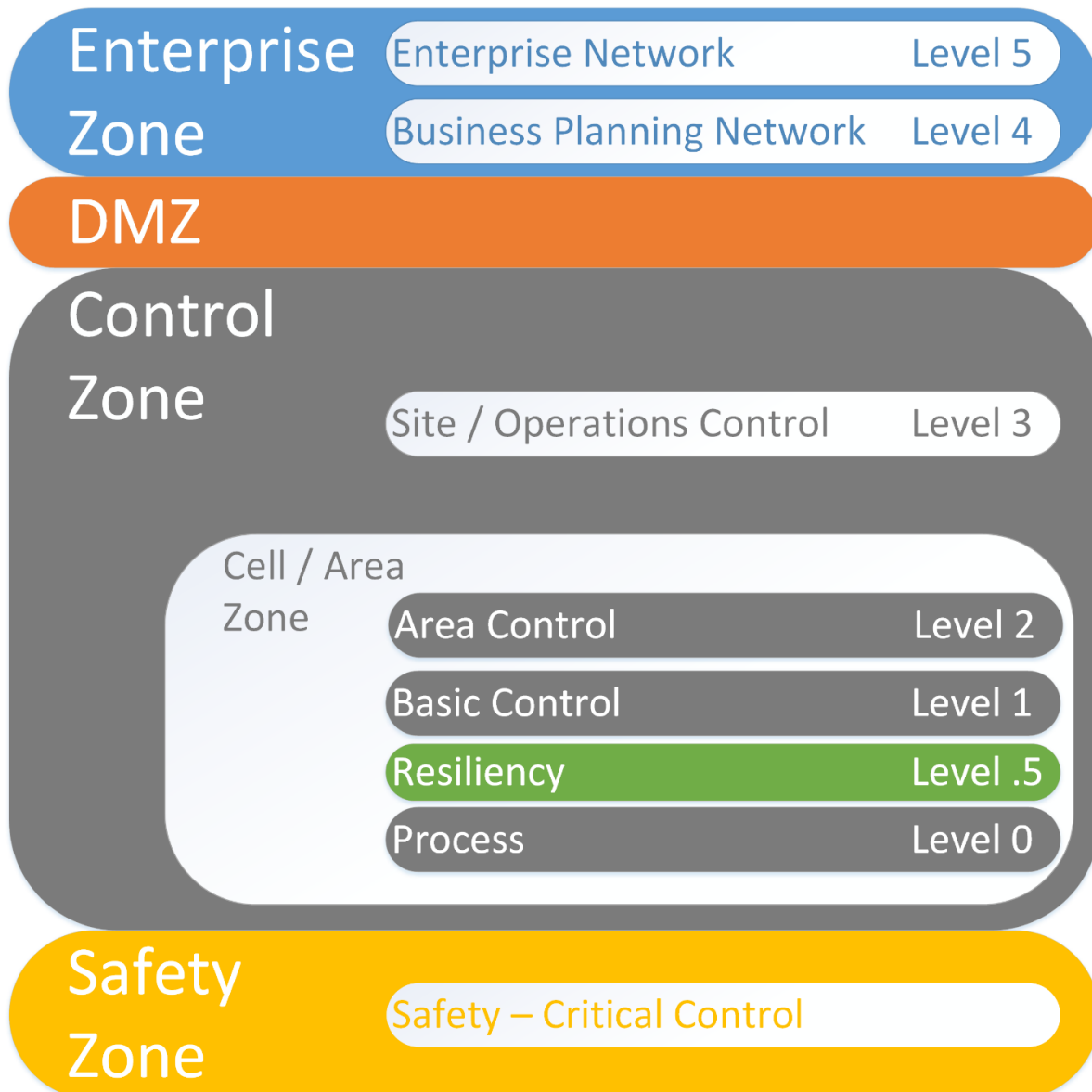


Figure 8: Modified Purdue Model for Control Hierarchy

The primary goal of the resiliency layer is to prevent a process from operating out-of-scope, and to return a process from a degraded state to fully operational. This differs in function to the safety zone, as its primary function is to bring a process that is operating out-of-scope back into scope, which includes but is not limited to, shutting down the process in the safest way possible. There is two-way communication between the safety systems, the controllers at Level 1, and the components at Level 0.

This Resiliency layer incorporates devices that utilize both hardware and software. These devices monitor the commands sent from a basic controller at Level 1 (such as a PLC) to a Level 0 device[s] (such as a motor or switch). It is looking for any command that is out-of-scope for the process. The out-of-scope command is a “bad” command that is outside of normal operating procedures, and can originate from anywhere (hacker, faulty device, random network traffic, etc.). If a bad command is seen by Level .5 devices, that command is not allowed to continue to the process equipment (Level 0). In which the Level .5 devices drop the bad command, and notify the basic controllers (Level 1) that a bad command was dropped, and a new in-scope command needs to be sent. Depending on the logic of the level .5 device, if bad commands continue to be seen, the Level .5 device can issue its own command to Level 0 equipment, initiating a predetermined degraded operating state. The degraded state will continue until an in-scope command changes the process, or if the safety systems take over. It is important to remember that the safety system is still monitoring the process directly, and that the resiliency layer does not replace the safety system. The following figures illustrate this process; showing the communication channels between the safety systems, Level 1, Level 0, and with/without Level .5.

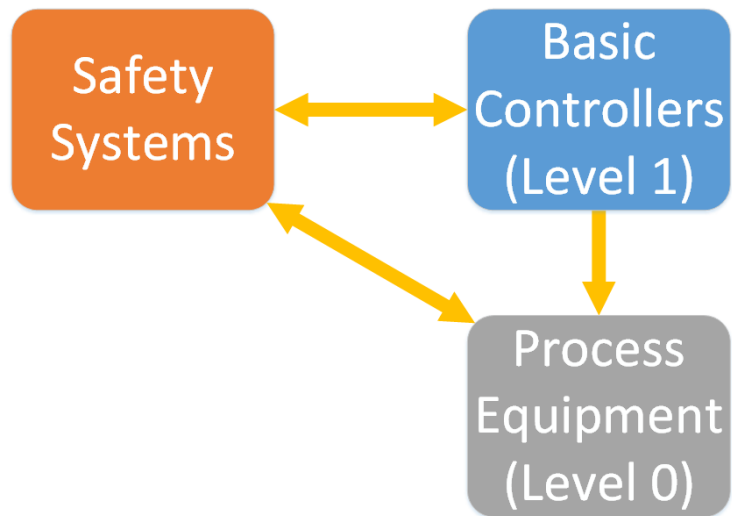


Figure 9: Communication Channels without Resiliency

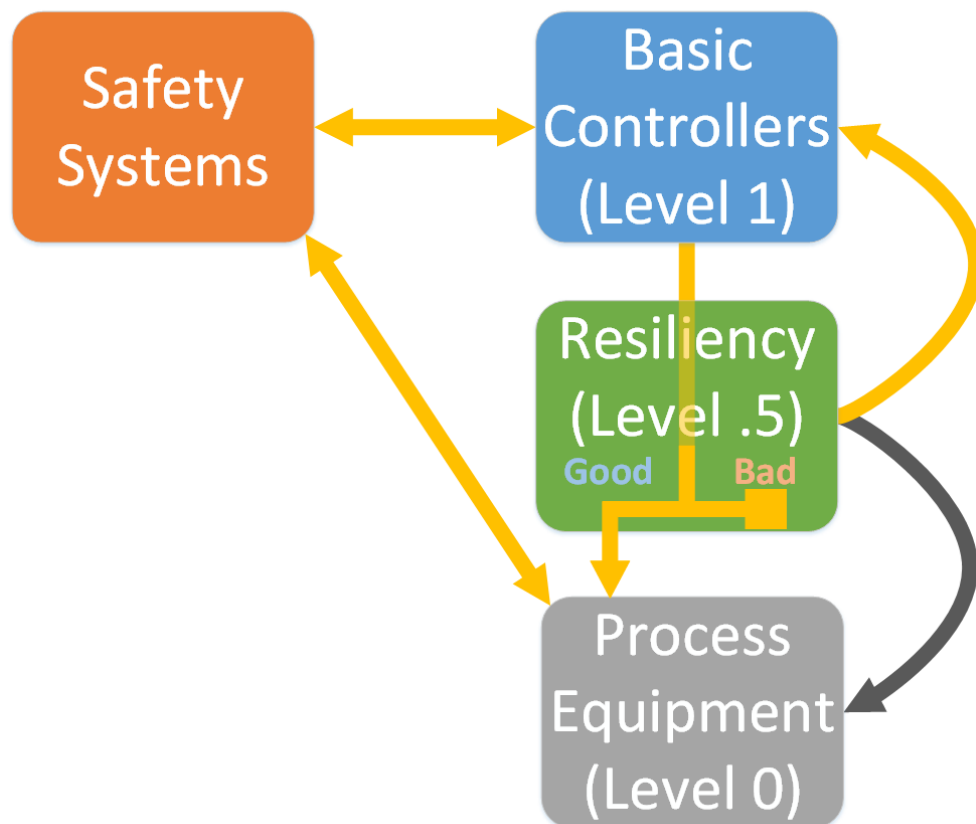


Figure 10: Communication Channels with Resiliency



Ideally, many Level .5 devices would be installed on a system, though this is not a requirement. A standalone device may be used depending on the complexity of the process. If many Level .5 devices are installed on a system with the utilization of communication between them, presumably along the conduits already in place, it would allow for higher influence being available on the underlying process. This communication could lead to predicting oncoming anomalies and taking the necessary actions to prevent or mitigate negative effects to the process. Communication will also allow for a process to continue functioning even if a certain percentage of Level 1 devices are damaged. For example, a process could continue to operate in a degraded state, even if 5% of the PLCs are damaged, due to the Layer .5 devices preventing the process from going out-of-scope. Communication between devices also allows for the resiliency layer to attempt recovering a process from a degraded state to fully operational. This area is ripe for automation, and eventually machine learning.

It is important that logging is conducted on Level .5 devices. The monitoring of these logs will allow for the discovery of indicators of attack (IOA) and indicators of compromise (IOC). IOA refers to monitoring the signs (indicators) of the steps that need to be taken by an attacker to compromise a computer system. (DeCianno, 2014) Examples of this include code execution, achieving persistence, and lateral movement. IOC refers to the digital evidence left behind on a computer system after an attacker has compromised said system. (DeCianno, 2014) Examples of this include malware and virus signatures, known bad IP address, and bad registry keys. (Chickowski, 2013) Monitoring these logs could help indicate if zero-day attacks are being used. Zero-day attacks refer unknown security vulnerabilities in hardware or software. (Symantec, n.d.)

To illustrate the resiliency layer in a real-world application, let's take a look at a traffic light system at a single intersection. To simplify the example, the system will consist of one HMI

(Level 2) that controls one PLC (Level 1), in which the PLC controls the light switch (Level 0). Most HMIs or PLCs will be coded in such a way to prevent out-of-scope commands from being sent to the traffic light (such as all green). This protection is only partial at best. It only prolongs black hat hackers from taking control and does nothing to prevent malfunctioning equipment (or other sources) that could send a signal that is interpreted by the light switch (Level 0) as all green. Installing a resiliency device looks at the commands going into the light switch (Level 0) and checks these commands against a table of known in-scope light configurations. This makes the system more resilient for numerous different scenarios. If for example lightning strikes the PLC (Level 1), in which it starts sending out commands for all green lights, the Level .5 device will prevent these commands from being executed. Also, when these bad commands are seen by the Level .5 device, a notification will be sent to the HMI that something is wrong with the system since multiple bad commands have been seen, and therefore tell the HMI to send an all blink red command. If redundancy is desired in the system, the resiliency device could be allowed to send the command directly to the light switch (Level 0), if the all blink red command is not sent by the HMI due to other issues in the system.

### Location, Location, Location

The primary reasons for choosing the location of the resiliency level in the Purdue Model for Control Hierarchy are: (1) this location has the most direct control over the process; and (2) this location is able to see and react to anomalies at the lowest level. The rest of this section explains why other locations in the Purdue Model for Control Hierarchy were not chosen.

The reason Level 1.5 was not chosen for the location to incorporate resiliency devices is because it does not protect the process from malfunctioning PLCs. For example, if a PLC is struck by lightning, and sends bad commands to Level 0 devices, Level 1.5 never sees these bad commands.

Anything above Level 2.5 was not chosen primarily because it is too broad of an area to implement resiliency devices. The traffic on this part of the network is higher than lower down the Levels. The resiliency devices are better utilized on a per operation basis. This will narrow the inputs/outputs necessary for resiliency devices to monitor.

The following figure is a basic ICS network diagram with the Modified Purdue Model for Control Hierarchy superimposed. (Byres, System Integration: Revealing network threats, fears, 2011) Operation #1 is shown with Level .5, while Operation #2 is shown without. This figure is a visual representation of why Level .5 is an ideal location to incorporate resiliency.

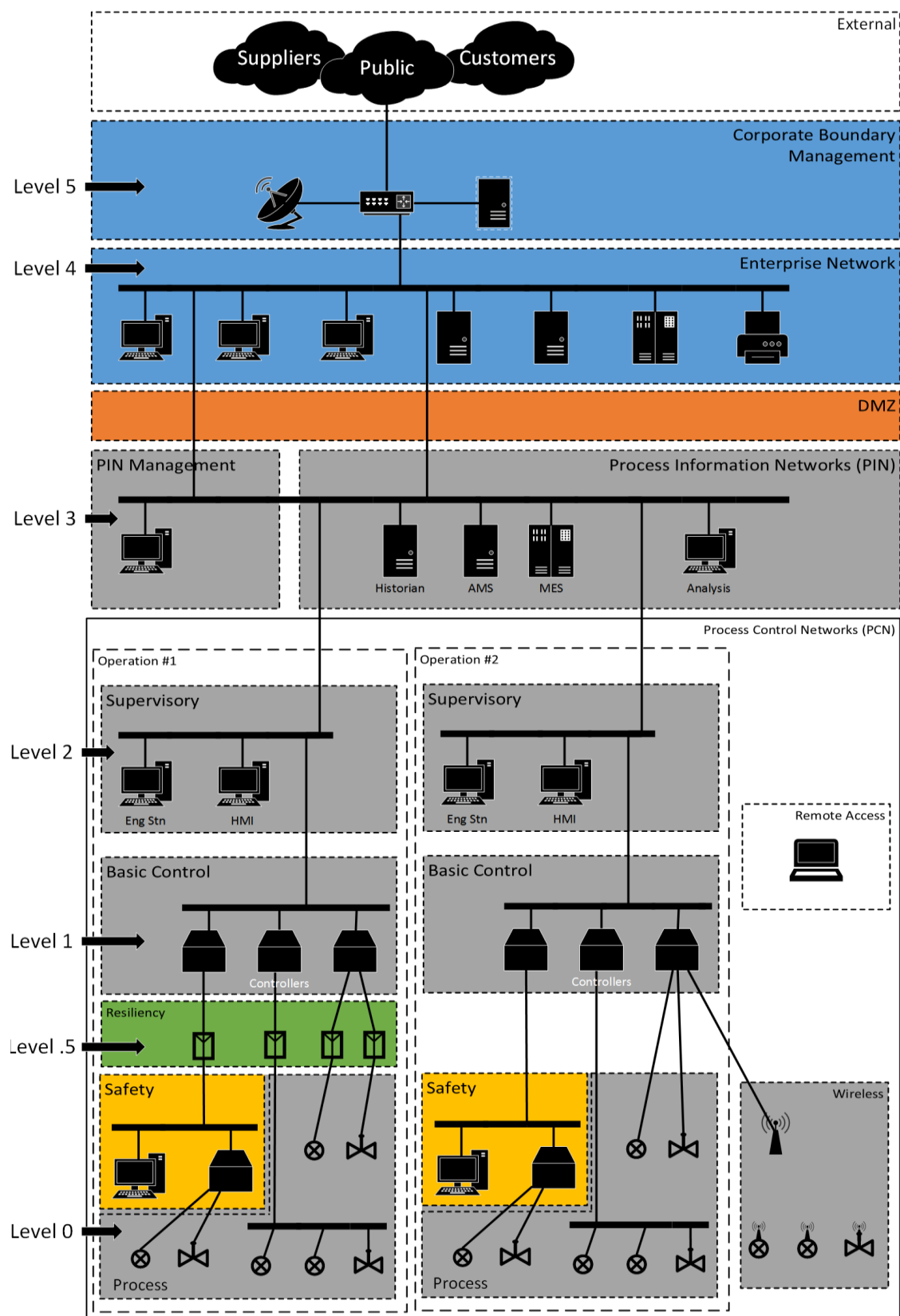


Figure 11: Modified ICS Network Diagram (Byres, 2011)

### Characteristics of a Resilient System

The addition of the Resiliency layer (Level .5) brings new characteristics to the system as a whole when implemented. As previously stated, most definitions of resiliency focus primarily on the characteristics. Fortification, antifragile, hardening, insensitivity, and resistance are just a few examples of various terms used in practice today. The characteristics used to define these terms tend to overlap in meaning as well.



*Figure 12: Example of Terms Typically Used for Resiliency*

To be consistent with the PPD-21, the characteristics we chose are Anticipation, Resistance, Adaptation, and Recovery. These characteristics are also not mutually exclusive. Meaning that the system can be in more than one state at any given time. For example, if a system is in the process of recovering, it is possible for the system to be adapting as well to be more resilient in the future. Below is a list explaining what each characteristic is.

- **Anticipation** – refers to anticipating disturbances and preemptively creating contingency plans for when a disruptive event happens. Red teaming and forecasting are just a couple of ways to achieve this.
- **Resistance** – refers to the ability of a system to be able to absorb or resist the impact when disruptive events take place. (Sansavini & Nan, 2017) In other words, to reinforce a system in such a way that performance deviations are minimized (or even negated), when the system is under duress. This includes situations when an attack is successfully executed against a system.
- **Adaptation** – is the ability of a system to adapt and change configuration or policy to prevent or minimize further performance deviations when disruptive events happen. Increased information sharing between critical infrastructure organizations will substantially help in this area.
- **Recovery** – refers to the ability of a system to return from a degraded state to a state that is within a preferred performance level. And then continue recovery until full capacity of the system is reached. In other words, how quickly a system can “bounce back” to its original working state. (Hyslop, 2007)

To illustrate where different term’s characteristics overlap, the following figure was created.

Anticipation	Resistance	Adaptation	Recovery
<ul style="list-style-type: none"> <li>• Planning</li> <li>• Preparation</li> <li>• Counter Measures</li> <li>• Contingency Planning</li> <li>• Forecasting</li> <li>• Preparation</li> </ul>	<ul style="list-style-type: none"> <li>• Withstand</li> <li>• Absorption</li> <li>• Robustness</li> <li>• Immunity</li> <li>• Dependability</li> <li>• Fault Tolerance</li> <li>• Protect</li> </ul>	<ul style="list-style-type: none"> <li>• Evolve</li> <li>• Strengthen</li> <li>• Adjust</li> <li>• Increased Capability</li> <li>• Respond</li> <li>• Resourcefulness</li> </ul>	<ul style="list-style-type: none"> <li>• Restoration</li> <li>• Regeneration</li> <li>• Repair</li> <li>• Renew</li> <li>• Rapidity</li> </ul>

Figure 13: Characteristics Overlap

Depending on the sophistication of the implementation of the Resiliency layer (Level .5), some or all of these characteristics will be seen. For a system to be considered resilient, it must

show signs of at least two of these characteristics. It is not enough for only one of these characteristics to be present.

There are three levels of how much resiliency is in a system. At a minimum with OT, a system must exhibit the Resistance and Recovery characteristic. And a

better resilient system will exhibit

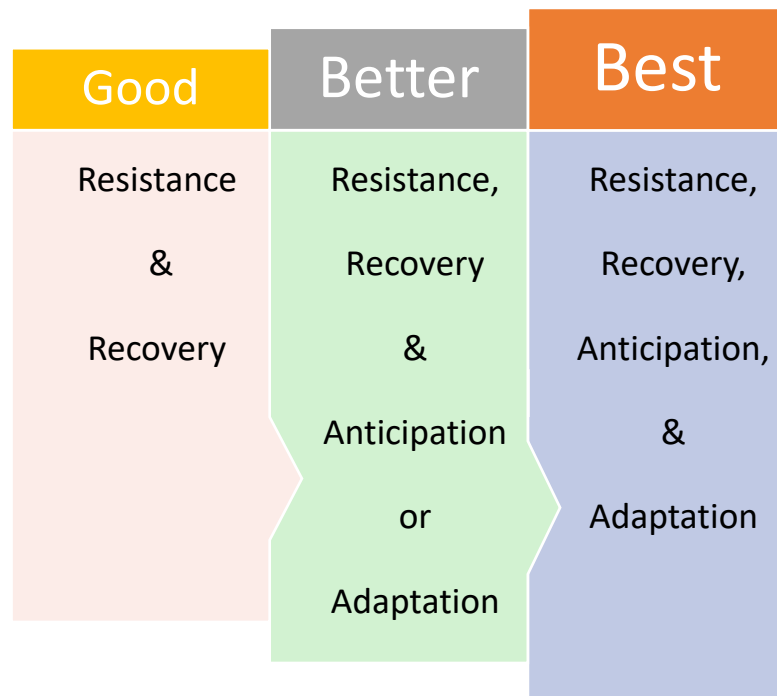


Figure 14: Good, Better, Best of Resilience

3 out of the 4 characteristics to some degree. For best results, a system will exhibit all 4 characteristics. An example as to why the minimum of Recovery and Resistance is necessary is as follows; let's take a system that is only able to recover quickly, but cannot resist abnormal conditions. Although the recovery aspect of resiliency is available, if the system is always down due to attacks (such as a DDoS attack), the recovery aspect is never utilized until the attack is done. But when the system is able to recover and resist an attack, the chances of the system going down are significantly decreased, hence the increased resilience.

### Prerequisites of a Resilient System

To truly make a system more resilient, one must first understand and model all the specifications of a system. This initial leg work must be completed thoroughly, for if one does not model the system properly, vulnerable points might be missed, exacerbated, or even created. The following is a non-exhaustive list of the data needed to successfully model a system.

- The most vital part of this analysis is to understand what systems are critical to the production process. "If everything is important, then nothing is important." (Collier, 2008) It also does not make sense to implement resiliency on non-vital systems first. A prime example of this is preventing hypothermia in a human body. When in extreme cold temperatures, focus should be kept on keeping the core of the body warm, as the core has all the vital organs necessary for one to stay alive. (Alvarez, 2015) If the best cold weather clothing in the world is used to protect the arms and legs, but the core is left vulnerable to the elements, eventual death of the body will ensue. If you switch the clothing to focus on the core and leave the arms and legs vulnerable, yes there is a



chance of losing an arm or leg to the elements, but the body will be less likely to shut down, and thus death potentially avoided.

- Map the interdependencies between the single system chosen and the other surrounding systems in a plant. In other words, identify how process inputs affect process outputs. This is necessary to fully understand what components of a system are vital to the process.
- Understand the limitations of the control systems used/implemented in the system. Most ICS are unique to the process they were built for. The capabilities, age, and brand are just a few factors that make the system unique. If your resiliency plan includes utilizing a PLC with an embedded firewall, and the PLC does not support this feature, that will create issues in the plan.
- Measure the normal operating conditions to create a baseline. If you do not have a baseline for normal operating conditions, it would be very difficult to implement a resiliency plan. Baselineing allows for the comparison of other states, to the preferred state as well.
- Map the range of acceptable degraded operating conditions. This helps with the design of a resilient system. A component of resiliency is if a system does fail, it fails well. If there are preferred degraded states, resiliency design can assist in guiding a failing system to one of these preferred degraded states. Failing states can include, for example, the percentage of PLCs that can fail before safety systems take over.

Typically, it is better to start with single processes or smaller system, and build from there. Big picture planning is vital, but it is easier to take baby steps, verify everything is functioning properly, and building from there, repeating the process to larger systems. It is unrealistic to make

an entire system resilient to all possible abnormalities. Therefor one needs to attempt an understanding what abnormality could take place, and how it could potentially happen. This risk assessment is a common principle taken directly from IS.

## Conclusion

CI is the backbone of our society and of utmost importance to national security. The interdependencies between the 16 CI sectors show how we need to make CI as a whole more resilient. Also, with the growing trend of IT/OT convergence and IoT, the attack surface area is growing exponentially. The need for more secure and resilient philosophies is needed for OT, as IT philosophies will not translate directly to OT. Therefore, a modification to the Purdue Model for Control Hierarchy is proposed. This allows for a more resilient control systems design. Once a resilient system is implemented, it will exert certain characteristics and traits. But before one can implement a resilient system, preemptive work must be completed. If nothing else, hopefully this paper contributes to laying the groundwork for further discussion and development of resilient framework or system design.

## Glossary of Abbreviations

BAS – Building Automation Systems

CI – Critical Infrastructure

DCS – Distributed Control Systems

DDoS – Distributed Denial-of-Service

DMZ – Demilitarized Zone

EEA – European Economic Area

EPCIP – European Programme for Critical Infrastructure Protection

EU – European Union

HMI – Human Machine Interface

ICS – Industrial Control Systems

I/O – Input and Output

IOA – Indicators of Attack

IOC – Indicators of Compromise

IoT – Internet of Things

IS – Information Security

IT – Information Technology

PII – Personally Identifiable Information

PLC – Programmable Logic Controller

PPD-21 – Presidential Policy Directive 21

OS – Operating System

OT – Operational Technology

RTU – Remote Terminal Unit

SCADA – Supervisory Control and Data Acquisition

US – United States

VPN – Virtual Private Network

## References

- Alvarez, D. M. (2015, January 26). *Chilling effect: How to prevent hypothermia*. Retrieved from Fox News Health: <http://www.foxnews.com/health/2014/01/06/chilling-effect-how-to-prevent-hypothermia.html>
- Assante, M. J., & Lee, R. M. (2015, October). The Industrial Control System Cyber Kill Chain. *SANS Institute InfoSec Reading Room*, 1. Retrieved from <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>
- Beal, V. (n.d.). *IT - Information Technology*. Retrieved from Webopedia: <http://www.webopedia.com/TERM/I/IT.html>
- Byres, E. (2011, June 30). *#1 ICS and SCADA Security Myth: Protection by Air Gap*. Retrieved from Tofino Security: <https://www.tofinosecurity.com/blog/1-ics-and-scada-security-myth-protection-air-gap>
- Byres, E. (2011, January/February). *System Integration: Revealing network threats, fears*. Retrieved from ISA: <https://www.isa.org/link/networkthreats/>
- Byres, E. (2012, September 5). *SCADA Security Basics: SCADA vs. ICS Terminology*. Retrieved from Tofino Security: <https://www.tofinosecurity.com/blog/scada-security-basics-scada-vs-ics-terminology>
- Chandra, M. (2015, June 1). *Industrial Automation And Control Systems Security*. Retrieved from LinkedIn: <https://www.linkedin.com/pulse/industrial-automation-control-systems-security-mithun-chandra>

- Chickowski, E. (2013, October 9). *Top 15 Indicators Of Compromise*. Retrieved from DARKReading: <http://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647?>
- Cisco. (2013, October 31). *Chapter: Converged Plantwide Ethernet Solution*. Retrieved from Cisco: [http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE\\_DIG/CPwE\\_chapter2.html](http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG/CPwE_chapter2.html)
- Cisco Systems and Rockwell Automation. (2008, July 22). Chapter: Solution Architecture. In *Ethernet-to-the-Factory 1.2 Design and Implementation Guide* (pp. 45-52). Cisco Validated Design. Retrieved from Cisco: [http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EttF/EttFDIG/ch2\\_EttF.html](http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EttF/EttFDIG/ch2_EttF.html)
- Collier, N. S. (2008, October 2). *If everything is a priority, then nothing is a priority*. Retrieved from NSCBlog: <http://www.nscblog.com/miscellaneous/when-everything-is-a-priority-then-nothing-is-a-priority/>
- Conklin, D. A. (2016). PowerPoint Slides.
- Control Services. (n.d.). *What is Building Automation*. Retrieved from Control Services: [http://www.controls-services.com/learning\\_automation.htm](http://www.controls-services.com/learning_automation.htm)
- DeCianno, J. (2014, December 9). *Indicators of Attack vs. Indicators of Compromise*. Retrieved from CrowdStrike Blog: <https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise/>

Department of Homeland Security. (2016, December 30). *Critical Infrastructure Sectors*. Retrieved from Official Website of the Department of Homeland Security: <https://www.dhs.gov/critical-infrastructure-sectors>

Department of Homeland Security. (2016, October 14). *What Is Critical Infrastructure?* Retrieved from Official Website of the Department of Homeland Security: <https://www.dhs.gov/what-critical-infrastructure>

Department of Homeland Security. (2016, December 30). *What Is Security and Resilience?* Retrieved from Official Website of the Department of Homeland Security: <https://www.dhs.gov/what-security-and-resilience>

European Commission. (2006, December 12). *The European Programme for Critical Infrastructure Protection (EPCIP)*. Retrieved from European Commission Press Release Database: [http://europa.eu/rapid/press-release\\_MEMO-06-477\\_en.htm](http://europa.eu/rapid/press-release_MEMO-06-477_en.htm)

European Union Institute for Security Studies. (2016). *Space Security for Europe*. Paris: ISSUE. Retrieved from [http://www.iss.europa.eu/uploads/media/Report\\_29\\_Space\\_and\\_Security\\_online.pdf](http://www.iss.europa.eu/uploads/media/Report_29_Space_and_Security_online.pdf)

Hyslop, M. (2007). *Critical information infrastructures: Resilience and protection*. Springer Science & Business Media.

KMC Controls Inc. (2013, May 19). *Understanding Building Automation and Control Systems*. Retrieved from KMC Controls: [https://web.archive.org/web/20130519124213/http://www.kmccontrols.com:80/products/Understanding\\_Building\\_Automation\\_and\\_Control\\_Systems.aspx](https://web.archive.org/web/20130519124213/http://www.kmccontrols.com:80/products/Understanding_Building_Automation_and_Control_Systems.aspx)

Krebs, B. (2016, October 21). *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*.

Retrieved from Krebs on Security: <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>

Kumar, N. (2017, February 2). *What is the difference between SCADA system and DCS?* Retrieved

from Quora: <https://www.quora.com/What-is-the-difference-between-SCADA-system-and-DCS>

Leyden, J. (2017, March 2). *We found a hidden backdoor in Chinese Internet of Things devices –*

*researchers*. Retrieved from The Register:

[https://www.theregister.co.uk/2017/03/02/chinese\\_iiot\\_kit\\_backdoor\\_claims/](https://www.theregister.co.uk/2017/03/02/chinese_iiot_kit_backdoor_claims/)

Obregon, L. (2015, September 23). Secure Architecture for Industrial Control Systems. *SANS*

*Institute InfoSec Reading Room*, 4-5. Retrieved from <https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327>

Palmer, D. (2016, October 25). *IoT devices can be hacked in minutes, warn researchers*. Retrieved

from ZDNet: <http://www.zdnet.com/article/iiot-devices-can-be-hacked-in-minuteswarn-researchers/>

Phillips, D. T. (2009, January 21). *Severe Space Weather--Social and Economic Impacts*.

Retrieved from Science@NASA: [https://science.nasa.gov/science-news/science-at-nasa/2009/21jan\\_severespaceweather](https://science.nasa.gov/science-news/science-at-nasa/2009/21jan_severespaceweather)

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, Understanding, and

Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems*, 21(6), 11-25.

Retrieved from <http://ieeexplore.ieee.org/abstract/document/969131/>



Rouse, M., & Haughn, M. (2016, March). *IT/OT convergence*. Retrieved from TechTarget:  
<http://searchitoperations.techtarget.com/definition/IT-OT-convergence>

Sansavini, G., & Nan, C. (2017, January). A Quantitative Method for Assessing Resilience of Interdependent Infrastructures. *Reliability Engineering & System Safety*, 157, 35-53. Retrieved from <http://www.sciencedirect.com/science/article/pii/S095183201630374X>

Shinder, D. (2001, August 28). *Understanding and selecting authentication methods*. Retrieved from TechRepublic: <http://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/>

Symantec. (n.d.). *What is a Zero-Day Vulnerability?* Retrieved from PC Tools:  
<http://www.pctools.com/security-news/zero-day-vulnerability/>

The White House Office of the Press Secretary. (2013, February 12). *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*. Retrieved from The White House President Barack Obama: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

Vijayan, J. (2013, February 14). *Obama executive order redefines critical infrastructure*. Retrieved from ComputerWorld:  
<http://www.computerworld.com/article/2494979/security0/obama-executive-order-redefines-critical-infrastructure.html>

Waterfall Security. (2016). *UNIDIRECTIONAL SECURITY GATEWAYS*. Retrieved from Waterfall Security: <http://waterfall-security.com/products/unidirectional-security-gateways>

Wavestone. (2015, October 18). *BruCON 2015 - Pentesting ICS 101*. Retrieved from SlideShare:  
<https://www.slideshare.net/Solucom/brucon-2015-pentesting-ics-101>

Wikipedia. (2017, February 2). *Operational Technology*. Retrieved from Wikipedia:  
[https://en.wikipedia.org/wiki/Operational\\_Technology](https://en.wikipedia.org/wiki/Operational_Technology)

Wikipedia. (2017, March 20). *Sneakernet*. Retrieved from Wikipedia:  
<https://en.wikipedia.org/wiki/Sneakernet>

Williamson, G. (2015, July 7). *OT, ICS, SCADA – What’s the difference?* Retrieved from  
Kuppingercole: <https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference>

Zetter, K. (2014, 11 3). *An Unprecedented Look at Stuxnet, the World’s First Digital Weapon*.  
Retrieved from Wired: <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

Zetter, K. (2016, March 3). *Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid*.  
Retrieved from Wired: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

THIS PAGE  
INTENTIONALLY  
LEFT BLANK