THE CYBER DEFENSE REVIEW

Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s

Author(s): Oz Sultan

Source: *The Cyber Defense Review*, Vol. 4, No. 1 (SPRING 2019), pp. 43-60

Published by: Army Cyber Institute

Stable URL: https://www.jstor.org/stable/10.2307/26623066

The Cyber Defense Review

Professional Commentary

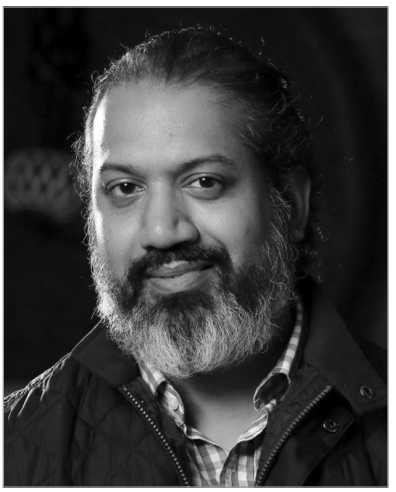
Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s

Oz Sultan

Over the past decade, social media has become an abusive component of the general media that we consume daily. In many cases, social media precedes and precludes traditional news mediums, by getting information out early or by providing detailed accounts of what is happening on the ground across the world.

What started out as social media users, influencers, and netizens capturing everyday happenings and reporting them in real-time (from 2007 to the present), evolved to include complex and organized propaganda systems by 2009. [1] Early propaganda systems involved state-sponsored propaganda sites presented as independent social media handles. State-sponsored disinformation began with Russian troll activism in Finland in the early 2000s. Infowar expert Dr. Saara Jantunen's book "Infosota", published in 2015, details the complicated networks of troll houses and blogs that constitute the concerted Russian infowar effort. [2]

In the first stage of the Ukraine conflict, Russia seized the Crimea, and Dr. Jantunen along with Finnish journalists and Finnish military researchers covering the conflict saw themselves slandered by a mixture of Russian trolls, Russian bots, and Russian disinformation blogs. Jessika Aro, one of the journalists investigating the trolls, was the most impacted as attacks targeted her home, phone, and workplace. [3] Finland has been able to keep Russia propaganda mostly at bay through legal attacks on the Russian disinformation campaigns that were run in-country by troll farms, [4] and by developing and supporting a compelling counter-narrative. [5] Finland's counter-narrative was launched in 2015 and is a top-down, bottom-up strategy that involved the engagement of 100 officials across various levels of government to analyze and map the spread of disinformation across their country. This strategic engagement included the participation of the FDR Center for Global Engagement at Harvard, for Finland to understand virality of disinformation. [6]



Oz Sultan is a tech, marketing and blockchain Industry veteran with 20 years' experience developing innovative solutions for brands and Fortune 100 companies. He is also at the forefront of American Muslim affairs, active in diplomatic and interfaith engagement.

Over the past ten years, Oz has leveraged social media signaling and analysis of trend and social media data to focus on Big Data analysis and how patterns can aid in solving complex problems. Oz has developed a Digital Anti-ISIS framework and counter-radicalization and disruption methodology for stopping online terror. In 2016, he was a counterterrorism, social media and Big Data advisor to the Trump Campaign. He is a regular contributor to i24 News, TexasGOPVote, The Ish, and Newsmax.

Oz currently consults in the Blockchain, Crypto, Cybersecurity and related CT arenas. He is a Board Member of the Homeland Security Foundation of America (HSFA); a Senior Fellow of the Council Board of Exchange; and a Senior Fellow at the National Minority Technology Council.

However, what the attacks on Finland have underscored is the larger Russian agenda to target western Europe – specifically Germany. The case of the false 'Lisa Story' in Germany from January 2016 is often cited as a textbook example of Moscow's modern information capabilities. Russian-language media reported allegations that a 13-year old Russian-German girl had been raped by migrants in Berlin before local authorities had time to verify the information. Those Russian reports were then picked up by mainstream news media in Germany and elsewhere. The false "Lisa Story" played out significantly across social media beyond Germany, most notably on Facebook, Twitter, and Reddit, where it was shared and re-shared with a significant impact. In the 'Lisa Case' we see evidence, for the first time, of several Russian elements of influence that are described in this article working in a coordinated way:

- A journalist from the First Russian TV channel picked up the case of the Russian-German girl and brought it to the main news in Russia;
- Russian foreign media like RT, Sputnik, and RT Deutsch reported on the case;
- Social media, as well as right wing groups, distributed the information on the Internet;
- Demonstrations were organized via Facebook involving representatives of the German-Russian minority (Deutschland Russen) as well as neo-Nazi groups;
- Russian foreign media in Germany reported from these demonstrations, which brought it to the German mainstream media;
- Finally, at the top political level, Russian Foreign Minister Sergey Lavrov made two public statements about his concerns about the inability of the German police and legal system to take such cases seriously because of political correctness. [7]

The evolution of Russian propaganda attacks from 2010 to 2015 was a testing ground for more massive campaigns launched against Germany and subsequently America. The false "Lisa Story" demonstrated how Russian propaganda stoked social media outrage and was supported by official disinformation that resisted challenges to the story with ambiguity, thereby rendering it as 'factual' in the minds of the audience it is intended to influence.

Understanding Online Propaganda and Amplification

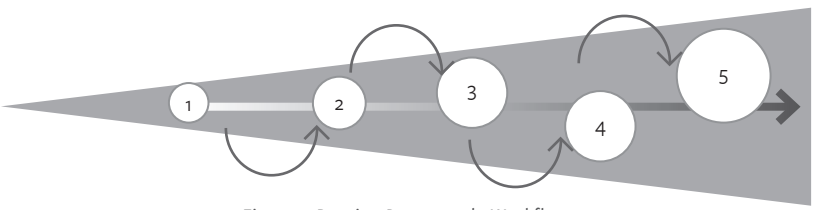


Figure 1. Russian Propaganda Workflow

The basic workflow of how Russian propaganda is developed, disseminated, and amplified is highlighted in Figure 1. The challenge with disrupting this workflow is one of a lack of preparedness on the part of many entities that are targeted: nations, politicians, corporations, and individuals. The steps of the Russian propaganda workflow are as follows: 1. Initiating incident (Lisa example) 2. Press or social validation 3. Foreign power amplification (Russian leadership commentary, for example) 4. Social buzz and shares 5. Social reshares and propaganda are taken by fact by people consuming it on social channels.

That the Russian model is partly leveraged by other state actors, such as Iran and China, which underscores the increasing challenge before the US and other democracies. We see conflation online between disinformation by state actors (and their respective social media strategies) and the difficulty of real-time media reporting. The latter is often becoming the tool of disinformation campaigns in their hurriedness to be the first to report. [8] The Defense Intelligence Agency (DIA) noted that:

> Russian intelligence services, including Russian military intelligence (GRU), have been increasingly involved in carrying out cyber operations abroad, as we have seen in the United States, in efforts to sway the 2017 French presidential election, and in attacks against Ukraine's power grid. The Kremlin is further developing these capabilities and its capacity to carry out information warfare, or what it calls "information confrontation." Moscow views control over the information sphere as crucial to influencing, confusing, and demoralizing an adversary, and the weaponization of information is a key element in Russian strategy. Russia employs a full range of capabilities, including pro-Kremlin media outlets and websites, bots and trolls on social media, search engine manipulation, and paid journalists in foreign media, to sway Western attitudes toward Russia and in favor of Russian governmental objectives. [9]

To challenge and disrupt Russian and state sponsored disinformation, as well as copycat campaigns leveraged by other foreign state actors, it is important to rapidly identify the false narrative stories. These are generally posted by a little known, unknown or subversive news/information site and mirrored in many languages across the Internet. These anchor stories, such as the "False Lisa" story, work like a signal that gets retransmitted through several repeaters. Disruption of these stories or weaponized content should actively involve the social media platforms that facilitate their dissemination. However, what we've seen in recent years is a reticence by Facebook, Twitter, Instagram, and WhatsApp to follow through.

If we are to be successful in countering the false narratives and propaganda, we need to be developing social media countermeasures and Standard Operations Procedures (SOPs) to parallel the deployment of personnel and ground communication systems. For forward deployed forces, this means developing a new social listening SOP that goes across traditional social channels (Facebook, Twitter, Instagram, Reddit, Snapchat, WhatsApp, Groupme, Voxer), new social channels (Telegram, Signal, Discord, Line, Kakaotalk, Weibo, Wechat, Coco, SOMA) and emerging crypto social channels (Steemit).

A simple model for analysis can be built upon the social mapping leveraging a tool like Gephi (https://gephi.org/) or Centrifuge (http://centrifugesystems.com/), which allow for an analyst to start mapping the social sharing across social networks and amongst power users or influencers. There are also a host of python and codeable tools out there, such as Graphtool (https://graph-tool.skewed.de/) and Carnegie Mellon University's GraphChi (https://github.com/GraphChi/graphchi-cpp). The key is to look for the 'social seed' or anchor piece of propaganda that started the sharing storm and then track where it jumped networks and who was endorsing it. Additionally, there are two factors that empirical analysis typically misses: velocity and popularity.

Velocity can be calculated based upon the speed by which a Tweet or series of Tweets spans different social graphs. Popularity is more imprecise math but can be roughly assessed by analyzing influencers (roughly 5k or more followers) and super influencers (approximately 100k or more followers) [these numbers also vary by network] that engage with or share the propaganda content. Generally, once you understand the amplifiers of specific types of propaganda, it becomes easier to develop a campaign through which you can respond to influencers or power users through sub-Tweets and structured social posts.

The challenge comes once the propaganda is picked up and spread by a mainstream news outlet and shared as either a 'story' or 'opinion' piece. This is further complicated by endorsements from Russian of other state agents or officials who are endorsing propaganda they issued in the first place.

From online propaganda to online terror

The modern terror recruitment network has moved beyond the 1980s, 1990s and early 2000's models of passing a terror training manual in the style of an 'Anarchist's cookbook' coupled with destination terror training camps. Beyond Russia, we are seeing parallels in online terror recruitment and influencing models. However, with terror recruitment, a piece of propaganda that is already widely disseminated or a terror attack that validates propaganda is used instead as a propaganda seed.

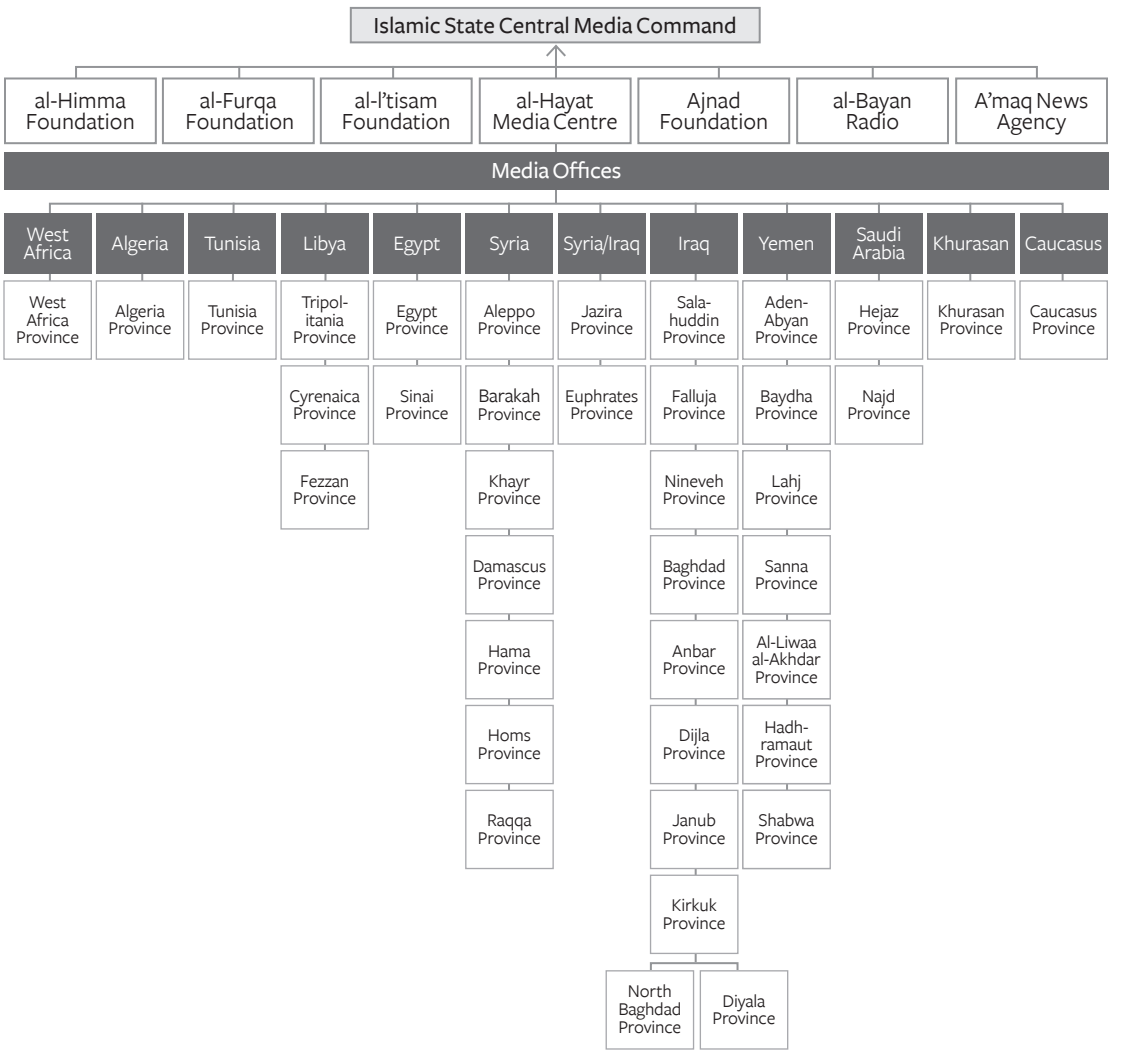


Figure 2. The ISIS Social Media Engagement Network Model (SEN) Source: Quilliam

ISIS's Amaq news agency has not only launched video and audio news but guides and training, as well. These are disseminated across a broad range of sites making suppression and remediation complicated. As of 2016, ISIS has been leveraging a complex content development and dissemination system coupled with online recruitment. The model below illustrates that Amaq and Al-Hayat – the most reported on ISIS news agencies, in the west, are only a small part of a vast network of online propaganda and influencing and recruitment efforts. As these networks are well entrenched across many conflict regions in EMEA (Europe-Middle East-Africa), while battlefronts change, the online presence persists.

Attacks by the US-backed Syrian Democratic Forces (SDF) in Syria have decimated ISIS Syria online operations, but many have just moved outside of Syria. Further, with the cross-pollination that has occurred between ISIS and al-Qaeda, cross-group insurgency is on the rise especially in complicated areas like Yemen and North Africa. SOPs for the assessment of ISIS and al-Qaeda related activities before ground incursions or tactical assessments should begin with a review of online engagement, which is made easier with tools like Livemap (https://isis.liveuamap.com/).

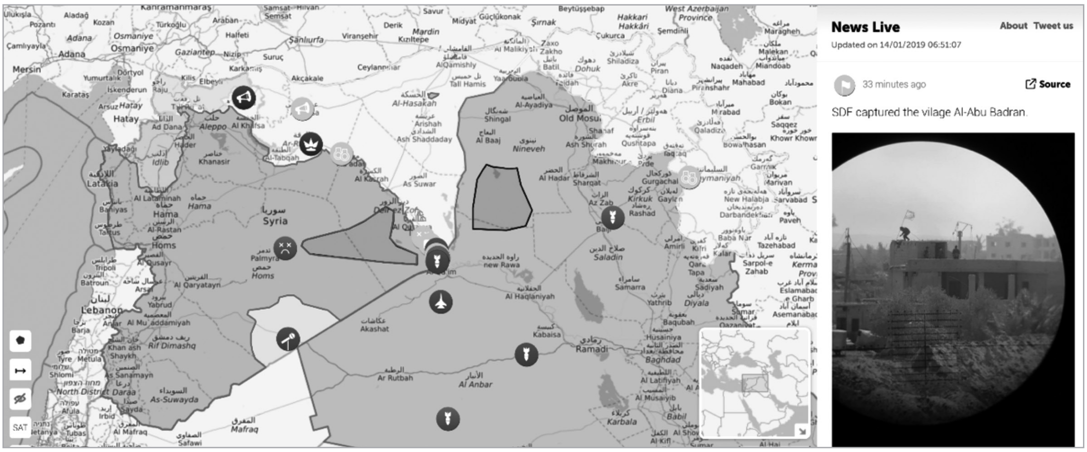


Figure 3. ISIS Social Engagement Network

Covering most of Middle East and North Africa, Livemap is a good start point in mapping what is going on in real-time, as well as what is being shared by ISIS and their SEM (Social Engagement Network). Social listening and mapping tools to understand where their propaganda is being disseminated are still necessary to map a specific incident. Typically, you can look to an attack or recent incursion and the messaging that is shared on Twitter, Telegram, and Signal. The challenge, however, is that the latter two social networks often have private groups that are invite only, which requires a bit of reconnaissance. Popular gaming platforms with chat on Xbox, PS4, and Nintendo Switch should also be kept in mind and analyzed based

on the frequency of gaming related tweets within a specific geographic arena. Generally, this is an indicator of where ISIS may be prospecting off social media networks, as well as areas for development of new SOPs.

Chatbots and Botnets

Chatbots and the development of automation bots in the 2000s have given rise to some unforeseen complexities, related to both social media and cybersecurity. What began as a method to automate volumes of standard responses to customers, as well as to provide an automated channel for customer engagement, has given rise to social media manipulation, distributed conversation attacks, and online mayhem. Similarly, Internet bots are automated programs that allow for the execution of a variety of tasks online have given way to networks of bots that can be rented like cloud hosting for any conceivable use under the sun.

The impact of these shifts is significant: In 2016, early ISIS botnets were deployed across Twitter [10] and operated much the same way as Russia, North Korea, and dark web hacker networks where attack networks can be rented, as easily as you or I could rent an Internet web service. In this environment, compromises range from simple scams across social media that request money or cryptocurrency [11] and then continue the scam to automated Distributed Denial-of-Service (DDOS) campaigns that leverage malware, brute force attacks, and propaganda dissemination.

DDOS Campaigns

In March 2018 Akamai reported that:

> On March 1, Akamai defended developer platform GitHub against a 1.3 Tbps attack. And early last week, a DDOS campaign against an unidentified service in the US topped out at a staggering 1.7 Tbps, according to the network security firm Arbor Networks. Which means that for the first time, the web sits squarely in the 'terabit attack era'. [12]

The significance of the power of these attacks means that we are now facing attacks that can overload and compromise network backbones and Tier 1 data providers. It is also the tipping point for the rise of DDOS attacks on the Internet of Things (IoT) and networked devices. Many of these new attacks target DNS or front-end web services, areas of the network that may be outsourced or less securitized in a cloud environment.

In 2003, I dealt with the rerouting of one million-page requests an hour through a home DNS server, after the Fortune 100 company I was working for experienced a catastrophic DNS failure. Had this option not been available, we would have looked at close to $1M in losses within a week. With new, cheap and difficult to trace Botnets, we now face rogue attackers who can erase their tracks, as quickly as they spooled up an assault.

Additionally, as IoT devices (which are mostly insecure or unsecured) start to become more mainstream, we face a new wave of risks that will affect every US military installation.

In many cases, it's not network deployed IoT devices (which need their own SOP) that are at risk for hacking; it is Bluetooth and PAN (Personal Area Network) attached devices like a Fitbit or an Apple watch or off-brand headphones with heart tracking that give away the location of military installations. [13] IoT devices are increasingly at risk for botnet hijacking. A secure protocol limits certain types of devices from FOBs but a more secure strategy is to develop SOPs that manage both networked and personal IoT risks.

Propaganda Dissemination

Similar to Russia's leverage of social media, the rise of bots within the social media ecosystem has had a chilling impact. As the propaganda models mature and become further decentralized across a broader geographic landscape, the risk is the speed and efficiency with which botnets can "vouch for" false narratives. A Tweet that starts as propaganda can be timed to be re-Tweeted and reshared by bot accounts that have thousands of followers and have been engaging in similar conversations for months before they are leveraged. If these accounts are not flagged or filtered they will continue to exist as a nexus that can share and reshare propaganda, false flag operations or disinformation.

Take for example propaganda bots impacts in Mexico [14] which have had chilling effects on influencing and shaping what people believe. The botnet phenomenon is also a technological leap in the impact of content dissemination and political or personal influencing. Consider bots as an amplification of the radio by a multiple of at least ten times. As botnets become cheaper, simpler to rent, and more accessible through cryptocurrency, a review of non-state and regional actors with social media fluency should be conducted to assess a threat baseline. Research teams that can analyze specific bots and bot attacks become extremely necessary as more organizations become impacted by bot attacks. [15]

When deploying social listening tools for active operations or assessing a given geographical landscape; once the general nature of daily conversations patterns is known and when propaganda shares can be tracked, it comes to either active disruption with owned or contracted social media handles, or a mass reporting action, which, while time-consuming, will deactivate the bot accounts. Another alternative to get a block of bots shut down rapidly is to work through representatives from Facebook, Twitter, Instagram, Telegram, Signal or other social platform's Fraud/Terror or Hate management teams.

Developing Digital Counter-terrorism (CT), IOT, Social and BOT SOPs

Bot technology is not a new thing. If we look back to punch card automation on IBM Systems and the architecture of virus software, we see a software process that can be automated to achieve the desired goal. The difference today lies with the number of bots, their coordination, and the efficiency with which they operate.

It is crucial to develop a SOP that accounts for bots and is a guide for specific types of bots within a known scenario. For example, if you want to prevent undesired social or data sharing of secure facilities or military installations, it may be necessary to require personnel to leave all personal IoT devices before coming to work or deploying. For cell phones and personal data devices, a VPN coupled with portable Faraday cages may be a simple solution to allow communications to their families and friends, while maintaining security. Why? Because if the Russians have started to ban their soldier's cellphones for fear of social media exposing deployments, we should be taking a few more cautionary steps. [16]

For SOP development, first, establish the scenario you need to protect. For example:

1) Restrict personal data sharing by personal, cellular or IoT devices on an installation or campus.
2) Eliminate the risk of hacking for network deployed IoT motion sensors deployed within a 5-mile radius.
3) Target a Russian or ISIS botnet operating within a specific theatre of operations.

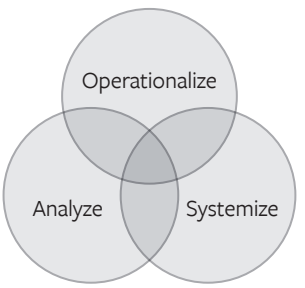


Figure 4. SOP Development

1. Analyze

For each scenario above, assess the following:

a. **Players:** Who is involved? Who is in command and requires reporting?
b. **Protocol**s: What are we trying to protect, defend against or prevent?
c. **Devices:** Are the IoT devices personal or public? What is the range of these devices? Who manages them? Who is responsible for securitization? What authorizations are needed?
d. **Bots:** Use standard network security SOPs to define penetration vulnerability for each scenario, for as many scenarios that exist.
e. **System:** Create a base protocol, process, stakeholders, escalation and implementation guide.

2. Systemize

a. **Define the boundaries:** Who does this impact? When does it need to be in effect? How will it be enforced? What are the compliance guidelines and the non-compliance ramifications?

b. **Establish the system:** Develop a basic guide; document and perform a test implementation. Iron out the kinks and repeat.

c. **Measure the results:** Establish metrics, cases for upgrades or modifications to the process and develop an approval process.

3. Operationalize

a. Deploy and perform a final test review.

b. Standardize across related or impacted operations.

c. Scale as necessary.

d. Perform periodic reviews to ensure the process is effective.

e. Assess metrics and report periodically.

f. Identify best practices that can be shared as SOPs for similar implementations or JSOC operations.

Cyber Risk Planning and Assessment

With the number of cyber-attacks and hacks that have occurred over the past 24 months, including the Marriott hack of 500 Million user accounts and recent compromises of critical infrastructure around the Tribune companies, it's time to start re-assessing risks from corporate civilian cloud infrastructure within the military and defense space. The NJCCIC (New Jersey Cybersecurity and Counterterrorism Information Cell) has noted the risks of China's Flusihoc bot network as well as those of, Iran, North Korea, and Russia. What last year's hacks underscore is an increased need to secure military systems that leverage cloud or public/hosted systems architectures. Those hacks also point to a change in the DDoS and Botnet attacks. Whereas previously, attacks were focused on disabling systems and locking data, these new attacks are designed to compromise cloud infrastructure and backend systems. [17]

The impact of this change is twofold. Instead of locking or stealing data, a successful attack could provide a foreign intruder access to critical publishing systems. As the social media and Russian propaganda machine have illustrated, this could prove catastrophic if it leads to mass dissemination of content. Consider the impacts during an election cycle or maritime conflict overseas.

The complexity of disinformation campaigns and hacks lead to threat scenarios that range from the risk of a news outage or a propaganda push during a foreign military campaign or attack. This is an increasingly real threat scenario that deserves further modeling, especially given China's recent militarization of the South China Sea.

To develop new SOPs for these risks, we need to establish cyber baselines, both for civilian linked and military deployed systems. Intel gathering from social media and public/dark web sources needs to become an ongoing passive process. Smaller attacks are often the precursor to larger scale attacks, and DDoS attacks need to be monitored to understand the trends of attack software and ransomware. Today it could be Ryuk, tomorrow, it could be reuse of WannaCry targeting unprotected medical devices or hospital infrastructure. [18]

Part of the problem is that across the U.S. Government and public technology infrastructure, we have a broad range of operating systems and control software ranging from early Windows and DOS variants to ACOE water table collection systems that still run on dial-up accessible UNIX systems. Healthcare and power generation systems add another layer of complexity, as they are easily targeted, and simply due to luck have not been the subject of a large-scale ransomware attack.

The US cannot continue down this perilous road. Security should involve assessing the age and penetrability of systems across a campus, FOB, enterprise, MAN (Metropolitan Area Network or City) or National/Global Network with rapid identification of unsecured network segments, as well as outdated or at-risk systems. This complexity will further increase with the development of Smart Cities that have layers of distributed IoT networks.

Smart Cities themselves will pose a more significant challenge, as the deployment of quantum computers improve the quality of life, reduce pollution and congestion, and extend major impacts to the battlefield of the future. This will bring a flurry of changes with the SOP process above and aid in planning. Cyber vulnerability assessment SOPs should follow existing and known protocols across military services, with updates made, at least quarterly, to the known universe of risk as well as new risks that stem from the overlap between military, MAN, developing Mesh power systems, cellular and civilian platforms and technology systems (social media, civilian to military-connected payment and data systems), as well as data vulnerabilities stemming from data stores of critical or vulnerable information.

The Cyber Risk Planning Ecosystem

Assessing the specific risk exposure for your scenario should begin with an analysis of your existing SOPs and a review of additional areas of concern that emerge from the risk ecosystem presented above. Full-scale cyber risk planning should involve a review of affected systems within your ecosystem – and the development of a mind map, as above. Once this is completed, begin with reviewing your systems risk, data risk, and then, personnel risks.

Lastly, by the mid-2020s, expect many legacy technology systems, databases, and platforms to begin or be at the end of their life. The ramping down and archiving of these systems presents a future risk, as simple hacking techniques such as "dumpster diving" when a hacker goes through a system's garbage can have major impacts if these systems are not sanitized and properly disposed of. The same applies to their data, which while less sensitive to you, may still be valuable to a less technologically advanced adversary.

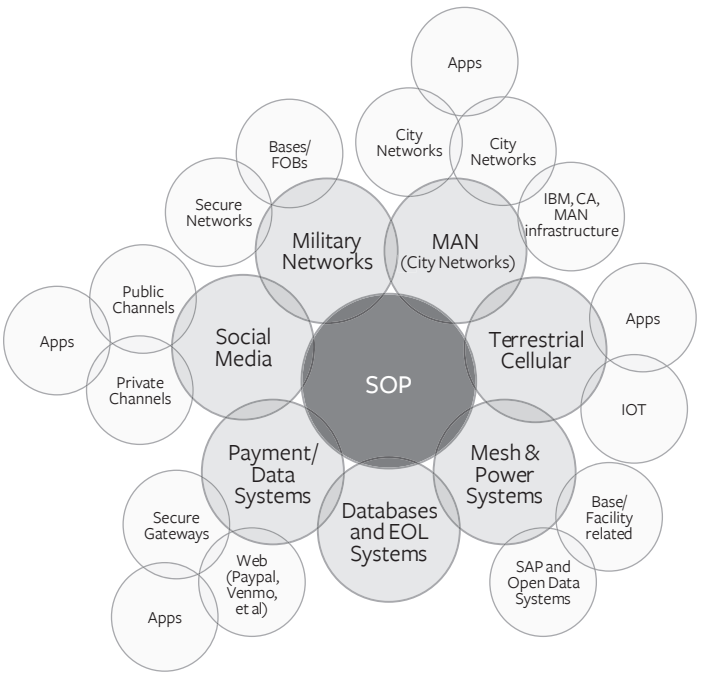


Figure 5. Risk Ecosystem

The Path from Cyber to Cryptocurrency

Cyber-ransom and cyber-attacks have rapidly opened the door between the cyber world and the crypto world. What began as global crypto-ransom attacks (WannaCry, Petya, NotPetya, Ryuk, et al.) [19] in 2016 and 2017 have given way to regular full-scale attacks across the Web, against the Web backbone, and even edge hosting services used for scaling to handle large customer requests.

The crypto world itself has also grown from a nascent environment of digital currency hobbyists to a multi-billion-dollar industry that will scale to the trillions, as developing countries begin reconciling their cross-border payments in Bitcoin and as large institutional players enter the market. This new market presents many opportunities and challenges as black-market transactions that have historically been done in cash have rapidly moved online and to the dark web.

The rise of crypto has also created cascading problems in human-trafficking, organ-trafficking and black-market sales of arms and embargoed goods. Iran recently presented a new dimension when they leveraged Bitcoin to bypass US sanctions. ISIS has long leveraged crypto to finance their insurgent operations across EMEA. Crypto exchanges themselves present another challenge as they are moving from startup style operations to larger scale daily transactions, so they are often subject to hacks and exposure, such as the release of information on 450,000 customers at CryptoMama. [20]

Global Crypto Implications

In South America, Venezuela has already begun settling cross-border payments with Bitcoin. [21] Several regional cryptocurrency systems have risen in Africa, facilitating both regional transaction systems and a reduction in cross-border payment expenses. Dubai has been focusing on a crypto trade zone that allows for Security Token Exchanges, while DATA [22] (US domestic Blockchain policy organization) is working with the Wyoming state government on both domestic crypto laws and the definition of crypto as currency. Simultaneously, Indonesia has moved to classify crypto as a commodity. [23] What does all this mean? The role that hard cash, black money, gold, and commodities played in the past is being rapidly challenged and replaced by digital currency and commodities.

The near-term implications of crypto are that new payment and commodity platforms are in play and need to be assessed as the world begins to move from paper and credit-based payment systems into digital payments and the Blockchain. The longer-term implications are yet to be determined. However, the global impacts of shifting currency and payment systems will alter how we conduct everything from remittances to forensic data analysis, to day-to-day operations across both civilian and military sectors.

The Blockchain

As China and Russia have challenged countries in EMEA, the US has begun to take steps to develop and deploy technology that moves it ahead globally. The Trump Administration has rapidly facilitated the assessment and development of Blockchain systems that will be evaluated within Opportunity Zones across the US, allowing for evidence-based research on a national scale. Within the military and civilian-related arenas – we need to consider the applications of the Blockchain, as well as the opportunities it presents both today and in the future.

Blockchain Use Cases

The Blockchain is simply a secure, immutable database that allows for transactions, queries, applications, and tools to be built while eliminating all middlemen and extra hands in the process. It creates is a system of trust that leverages frameworks (called smart contracts) which allow for process-based or automated transactions. The use cases for the Blockchain are infinite – as is the value that is created with new Blockchain deployments

and Blockchain systems. However, for simplicity sake, a few examples to clarify the value of Blockchains.

Weapons Management

Take for an example, the challenges of monitoring, tracking, and managing 1,000,000 H&K rifles deployed across several FOBs in three theatres. Today this is done with a mish-mash of technology and paper-based solutions that often tax both workforce and systems. Now consider a Blockchain based solution that was deployed leveraging an Ethereum or XYO based technology, which could place an encrypted, globally accessible tracking tag on every weapon. Then consider that the tags could be integrated to allow for missing, stolen or captured rifles to be deactivated or deauthorized from use. The system allows for constant inventory, management, authorization or archival and reduces cost, complexity, and workload.

Healthcare Records/Combat Medic Matching

In an operational theatre, access to a unit of blood or plasma can be the difference between life and death. While dog tags are useful, Blockchain technology could be used to not only manage and securitize military or civilian data but, in a crisis, combat situation or terror attack, could rapidly allow medics to assess the people around them to help save lives. Blockchain-based medical records could reduce the costs of Department of Veterans Affairs administration data by up to fifty percent while allowing the military secure, lifetime access to their records, which only the patients themselves could delegate or allow access.

Refugee and International Detention Coalition (IDC) Management

Joanne Herring has one of the few success stories in Afghanistan, called the Herring Plan, where her policies allowed for successful development and protection of small cities. By creating a five-factor city development program in Khairabad, Afghanistan, Herring aided the refugee and border conflict infrastructure development. Adding a Blockchain based system would ease city growth and allow for the organized management of city infrastructure, people, systems, and payments.

Matthew "Griff" Griffin with Combat Flip Flops is another dramatic story. The continuing problem both faced with the inability to document displaced populations and refugees. Worse, displacement and separation allow for continual child soldier conscription and human trafficking issues (e.g. ISIS and Boko Haram). A Blockchain based identity solution could solve everything from identity management to the resettlement of people and return of assets following the cessation of a conflict.

Food Safety and Supply Chains

Poisoned food has killed thousands and is the tipping point of global food chain problems. As global weather changes, sea levels and inclement weather become larger concerns, safety and provenance of the food supply become more critical. Blockchains are poised to begin solving these challenges. [24]

Base/City/Opportunity Zone Management

The 2020s will see the development of Smart Cities and technology systems that will both deliver information and services while generating exponential quantities of data. Blockchain-based systems will allow for these data systems to work interchangeably and aid in economic development where data becomes the new oil. Additionally, moves by the NMTC to develop national (US) Blockchain standards will start driving new consensus, audit and identification technology by 2020.

Combatting Weaponized Internets

Russia is already planning an alternative Internet [25] while China is dabbling in its Internet infrastructure with a prediction that it will split by 2028. [26] Developing a Blockchain based Internet protocol tied to IPv6 or DNS or a new paradigm would easily allow us to combat digital foes that focus on manipulating information and access. Blockchain stacks like Prasaga will become newer models for data transport across networks on trillions of data connected devices.

Preparing for Future Risks – After ISIS and on to the "Laughing Man"

From Russian adversaries who have leveraged propaganda to accomplish everything from seeding discord in the Middle East to propaganda as news today, we have seen both risks and threats evolve. Today's terror threats of ISIS, AQIS (al-Qaeda in the Indian Subcontinent), Boko Haram, Al-Shabaab, and regional terror networks, funded by ISIS and al-Qaeda, will give way to evolving modes of terrorism once ISIS in Syria falls.

While insurgents can be killed – ISIS and Al-Qaeda's warped cult ideology resides online, in the dark web, and as PDFs and magazines that are passed among the disenfranchised in online forums. ISIS's focus on Europe in the past indicates that there is a risk of ISIS attacks across NATO countries. Recent ISIS suicide attacks on Iran's Revolutionary Guard and India's military have retrenched hostilities between the two and Pakistan, who in 2019, is still ill-equipped to tackle local insurgents, ISIS-linked terrorist groups, and emerging groups seeking regional hegemony.

Online bot and cyber-attacks are now beginning to see IoT compromises come to light. Couple this with the risks of Fitbits and App-connected devices and cellphones and there is a new need to understand that civilian hacking has entered the military realm. Social media is not only a threat to troops; it is a geo-taggable beacon that can share a secret base location on Instagram. Worse, researchers have been able to use simple tech and social media to misdirect NATO troops to ignore their orders. [27] Cryptocurrency and cyber-attacks have become synonymous while healthcare systems, including MRIs, are as susceptible to viruses and attacks if their systems are not secured or firewalled before they connect to a network.

Technical and critical system SOPs need to be reviewed and have quarterly refreshes, at a minimum, as the rate at which risks are changing accelerates every year. We are in an era when moving from defined and known enemies to amorphous groups (ISIS, ANTIFA, race supremacists) to individuals and smaller groups hidden by various online personas whose technology and cryptofinance knowledge makes them as dangerous as larger groups. We have begun to classify these latter groups and individuals as the "Laughing Man" or "Laughing Men" as their motivations tend to be a subset of a larger, more organized adversary.

These adversaries comprise the new range of international actors, domestic terrorists, and threats that technology, cryptocurrency, and changing digital and physical battlegrounds are beginning to produce. This landscape will also face rising challenges from Russia, China, Iran, North Korea, and regional African actors, none of whom will slow down their attacks if their propaganda machines have an impact. Instead, "Laughing Man" or "Laughing Men" will define the new ways in which we must develop our defenses. Lastly, consider the opportunities of the Blockchain and the opportunities for the US to think beyond how it operates today while tackling the challenges of tomorrow.

NOTES

1. https://doi.org/10.1177/1461444809105345.
2. https://yle.fi/uutiset/osasto/news/finnish_researcher_russia_ramping_up_its_information_war/8385245.
3. https://www.smh.com.au/world/finnish-journalists-jessikka-aros-inquiry-into-russian-trolls-stirs-up-a-hornets-nest-20160311-gng8rk.html.
4. https://www.dw.com/en/court-in-finland-finds-pro-kremlin-trolls-guilty-of-harassing-journalist/a-45944893.
5. https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.
6. Ibid.
7. https://www.nato.int/docu/review/2016/also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm.
8. https://www.washingtonpost.com/news/arts-and-entertainment/wp/2017/06/27/the-cnn-retraction-and-the-danger-of-relying-on-one-anonymous-source/?utm_term=.8a871f513283.
9. http://www.dia.mil/News/Speeches-and-Testimonies/Article-View/Article/1457815/statement-for-the-record-worldwide-threat-assessment/.
10. https://propagandacritic.com/index.php/case-studies/isis-botnet/.
11. https://www.newsbtc.com/2018/08/10/researchers-identify-15000-strong-botnet-scamming-crypto-twitter/.
12. https://www.wired.com/story/creative-ddos-attacks-still-slip-past-defenses/.
13. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.
14. https://medium.com/@erin_gallagher/propaganda-botnets-on-social-media-5afd35e94725.
15. https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/daswani/daswani.pdf.
16. https://www.bbc.com/news/world-europe-47302938.
17. https://www.cyber.nj.gov/threat-profiles/botnet-variants/flusihoc?rq=china).
18. https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#18c765b9425c.
19. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.
20. https://www.ccn.com/breaking-major-crypto-brokerage-coinmama-hacked-450000-users-affected-in-massive-worldwide-breach.
21. https://smartereum.com/4791l/bitcoin-latest-update-argentina-accepts-payment-for-goods-sold-to-paraguay-in-bitcoin-btc-bitcoin-news-today-btc-usd-price-today/.
22. https://theish.us/wyoming-data-and-the-gold-rush-of-coming-crypto-regulations-4c3c06cd331d.
23. https://bitcoinexchangeguide.com/bitcoin-officially-classified-as-a-commodity-within-indonesias-borders/.
24. https://channels.theinnovationenterprise.com/articles/blockchain-set-to-solve-the-fake-food-problem.
25. https://www.dailymail.co.uk/sciencetech/article-5126931/Russia-plans-create-independent-internet-2018.html.
26. https://futurism.com/google-future-china-internet.
27. https://www.businessinsider.com/officials-tricked-nato-troops-into-disobeying-orders-with-social-media-20192.