NETWORK CONTAGION:

LESSONS FOR CYBER SECURITY PROFESSIONALS FROM COVID-19

BY COREY HIRSCH

ontagion, the rapid uncontrolled spread of invisible infectious agents from host to host, occurs in biological and electronic networks via parallel mechanisms. Similarities, and important differences, between biological pandemics and cyber outbreaks, can inform defenders of both kinds of networks.

During outbreaks, defenders choose strategy and tactics. Without advanced technology it may not be possible even directly to detect and recognize the presence of the malicious agent. This agent, whether coded in RNA, or C++, is turning our machinery to its own ends … including its own replication and dispersal, wreaking havoc on our network. We'll need a 'sequence', or a 'signature' to define uniquely the enemy's presence and give it a name.

Defenders encounter ethical dilemmas, ranging from how many dollars would it be worth to mitigate this outbreak slightly more fully, or slightly more quickly, to how much privacy should be sacrificed in the pursuit of reduced contagion? Will we adopt John Stuart Mill's premise of seeking to maximize the aggregate good, or Kant's of adherence to a core set of ethical principles? When choosing strategy and tactics, defenders need to apply beliefs on which services are 'essential', and which could be acceptably tactically interrupted.

1) Could experience gained responding to cyber outbreaks such as WannaCry and NotPetya inform public-health decision makers on:

   Optimal policy on economic re-opening following Covid-19 lockdown; should it be governed locally, regionally, or nationally?

2) Could experience gained responding to Covid-19 guide cyber security professionals on:

   Developing Enterprise Network Defense tactics analogous to containment and mitigation?

3) And where these domains overlap:

   How can cyber security professionals craft strategy for defense of newly home-worker-based employee networks from Window's SMB3.1.1 vulnerability?

Parallels:

Networks comprise a defined and bounded population of connected hosts. In pandemic terms, a network, that is a human population within a public-health zone, is usually bounded by a geographical perimeter, often a political or legal boundary. In a computer network, the population of included machines is bounded virtually, by connectivity map position relative to a firewall, usually independent of physical location. In both types of networks, some hosts are more inter-connected than others. In pandemics these are 'super spreaders'; highly-connected hosts with a high rate of transmission. In cyber networks, some machines, such as Domain Controllers, are highly-connected, and prone to afford attackers a nexus of contagion.

Biological pathogens comprise *viruses*, such as SARS-CoV-2, the virus that causes Covid-19, *worms*, *bacteria*, *protozoa*, and *funghi*. Each has distinct form, function, attack chains, and generally ***emergent*** attack strategies. They are infectious agents undetectable directly by our 5 senses.

In cyber networks, threats are categorized by form and function; *viruses* and *worms*, named for similarities to their biological name-sakes, and *Trojans*, *adware*, *spyware*, other forms of malware, and attack chains such as 'APT' (Advanced Persistent Threat), 'BEC' (Business Email Compromise), 'ART' (Advanced Ransomware Threat), 'DDoS' (Distributed Denial of Service), and others. They are infectious agents, and undetectable by our 5 senses. Cyber-attack strategies are generally ***crafted***. Cyber-attack and defense strategies may mirror those in biological networks.

Some microbes are beneficial, others disease-causing. Some external code running on our host is helpful, other code can spread ruin on our organization.

Identifying 'friend' from 'foe' is a central activity of biological and electronic immune systems. A genetic 'sequence' serves as avatar of a biological virus; a 'signature' likewise for malware. Defenders catalog these *indicators of compromise*, and devise systems to block, kill, or neutralize the attacker. This approach is referred to as 'blacklisting', or 'deny-listing'.

Allowing connections that are known to be benign, and only those, is referred to as 'whitelisting', or 'allow-listing'. This is a stronger security posture, since anything not known to be benign, so anything *unknown*, is disallowed.

A healthy human, or a growing company, likely has an appetite for new contacts. New friends, new suppliers, customers, investors. Allow-listing too strongly, in normal times, can stymie other

organizational objectives. However, when it's time to hunker-down, and survival is the objective, a shift along the spectrum towards allow-listing reflects this shifted risk appetite.

July 16, 1945; ***Trinity Test***, the first atmospheric atomic explosion, in White Sands, New Mexico. Prior to Trinity, Edward Teller, often referred to as 'Father of the Hydrogen Bomb', and one of the lead physicists on the Manhattan Project, was concerned that this test would ignite nitrogen in Earth's atmosphere in an uncontrolled nuclear chain reaction. He feared ***cataclysm by fire.***

Sidebar 1

Pathogens meet their hosts thru ambient contact, where the host meets the environment, such as in respiration. Where oxygen and carbon dioxide are exchanged, broad contact surface in the lungs and *respiratory tract* provides an attack vector to pathogens such as SARS-CoV-2. In companies' electronic networks, these are *web services*, the broad surfaces where exchanges with the environment occur.

Pathogens may also meet their new hosts thru ingestion, such as via *contaminated food or water*. Companies ingest malicious code as well, through ingestion of *malicious email and corrupted software files*, for example. And pathogens may gain entry through a hole in the firewall, such as a *cut or scratch* in the skin. Likewise, a USB key dropped in the parking lot may make its way into the facility, and onto the network via a *host's USB port*.

Vaccination can be seen as a beneficial '*social engineering*' strategy in protecting a biological network, as the host's immune system is tricked by the vaccine into building antibodies which will later prove useful in defending against a specific pathogen. Vaccines serve a similar function biologically as patches in computers, creating immunity in one host from a particular vulnerability.

Biological viruses' emergent strategies may rely on humans touching their faces with unwashed hands. Defense can therefore take the form of either washing hands, or not touching faces, or both for defense-in-depth. Computer viruses' crafted strategy may rely on humans inserting found USB keys into their computers. Defense can correspondingly be either 'washing' (scanning) the USB key, or preventing its insertion into the computer.

Pathogens spread via physical processes, often via processes of *sharing* or *exchange*. Cholera, originally thought to spread via shared air supply, was shown by Dr. John Snow to spread via shared drinking water supply. SARS-CoV-2 is believed to spread via exchanged respiratory droplets, airborne, or on surfaces. Malware generally spreads via *exchanges* or *shares*. It spreads through exchanges of packets, code or data, between hosts across a network, such as Ethernet, or through sharing of malicious files, in a shared file structure. Both methods can be employed simultaneously. For example in June of 2017, NotPetya propagated through network-based delivery of compromised application patch files.

Pathogens' transmissibility and severity vary. Measles' transmissibility, expressed as R0 (R naught) is high at 15, while its mortality rate is 0.2%, compared to Ebola's transmissibility at 2, while its lethality is high; 71% of those infected will succumb, according to the WHO, for the Sudan strain. Malwares' transmissibility varies as well. In the WannaCry outbreak of May 2017, 'R0' was high

since the underlying vulnerability, Eternal Blue, allowed for rapid one-to-many transmission, to connected at-risk hosts, without user action required (i.e. 'wormable'). Three hundred thousand internet-connected machines in 150 countries were infected in 9 hours.

The CVE system, Common Vulnerabilities & Exposure, for cataloguing and rating vulnerability's severity ('lethality'), rates the Eternal Blue CVE known as 'SMB1' (Server Message Block CVE 2017-0144) at 8.1 on a scale where 10 is the maximum.

Transmissibility generally has grown in both domains in recent decades. The advent and growth of internet connectivity, presently estimated at 31billion devices, has exponentially increased cyber-risk exposure, while the growth of air travel, and travel generally, has had a parallel effect in pandemic risk, placing much of the human population of Earth, 7.6 billion, in range of pandemic.

Outbreaks in both domains may be tracked with global heat-maps illustrating where contagion is active. Such maps, for example the John Hopkins University CoVID-19 Distribution Map (https://www.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6), and the European Union Agency for Cyber Security WannaCry Distribution Map (https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst), are similar in appearance statically, and dynamically as outbreaks progress. Outbreaks in either domain trigger financial distress.

Epidemiologists and health care professionals, as well as CISOs and cyber security incident responders, rely on testing, and deal with false-positives and false-negatives. Both types of teams deal with 'signatures'. In diagnostic testing, these indicate the presence of a dangerous type of coded information, for example the Visual C++ V6 coded WannaCry Ransom-worm, or the RNA code of SARS-CoV-2. In serum, or forensic, testing, a historic picture of contagion is available.

April, 1963; American novelist Kurt Vonnegut, who was 23 years old during the atomic attack on Hiroshima, posits a crystalline structure for ice, stable at room temperature in his novel *Cat's Cradle*. A single seed crystal of ***Ice Nine***, upon first contact with liquid water would replicate itself, instantly freezing solid all water on the Earth, causing the destruction of all life. Vonnegut feared ***cataclysm by ice.***

Sidebar 2

Both types of teams employ hybrid defense schemes in a defense-in-depth layered approach.

Outbreaks in either domain may 'leak' into the other. Studies have shown that hospitals which have suffered ransomware attacks have higher rates of patient mortality, for example. WannaCry led to adverse health outcomes in UK, when the function of the NHS (National Health Service) was severely impaired. Conversely, during the Covid-19 outbreak, levels of 'phishing' attacks have been elevated several-fold, 667% in March 2020, according to KnowBe4, and more than 100,000 malicious domain names containing 'Covid' have been registered in support of cyber-crime campaigns.

If, on top of the societal disruption caused by Covid-19, a WannaCry-type outbreak were to occur, this would be a compounded nightmare scenario. It would effectively disable the home-working, remote-learning, and online-shopping coping mechanisms that have cushioned this lock down, socially and economically. Moreover, cyber recovery would be impeded as many infected machines would be away from the office, as would many IT resources. If the internet were impaired, the ability to remediate these machines remotely would be further hampered.

Planning for the defense of biological and cyber networks involves defining and executing steps that reduce the *likelihood* of compromise, and steps which minimize the *impact* or consequences, should it occur. In addition, good defense posture includes enhanced ability to *recover* effectively afterwards.

Risk management in both domains involves assessing the threat environment, designing and executing aligned strategies to minimize the aggregate multiplicative product of the *likelihood* of compromise, and its potential *impact*.

To execute cleanly a sound strategy in either domain, true and relevant information is essential. In the Covid-19 pandemic for example, shortages of PPE (personal protective equipment) for health care workers, and other important medical assets, are a concern. Some pandemic hotspots have set up hospitals specifically for Covid-19 treatment, and others for non-Covid-19 case work.

This is a strategy which cyber professionals would refer to as '*enclaving*'. There may be opportunities for improvement in its execution recently in the US based on additional information. If it were known which health care workers had achieved Covid-19 immunity through prior exposure, the shortage of PPE, and qualified health care professionals, could perhaps be alleviated by assigning immune health care workers to the Covid-19 specialized facilities. This information may be knowable, via diagnostic, and/or serum testing. *Surveillance*, in epidemiology, and *monitoring*, in cyber defense, are essential foundational activities.

Enclaving, that is walling off a set of hosts with a common set of attributes, may form an element of the right approach to the first of our three questions. Enclaved hosts may be those with similar levels of *information trust* requirement, or a similar set of *functional* requirements. From a risk management perspective, they may be hosts with a similar *likelihood of compromise* profile, or a similar *impact of compromise* profile.

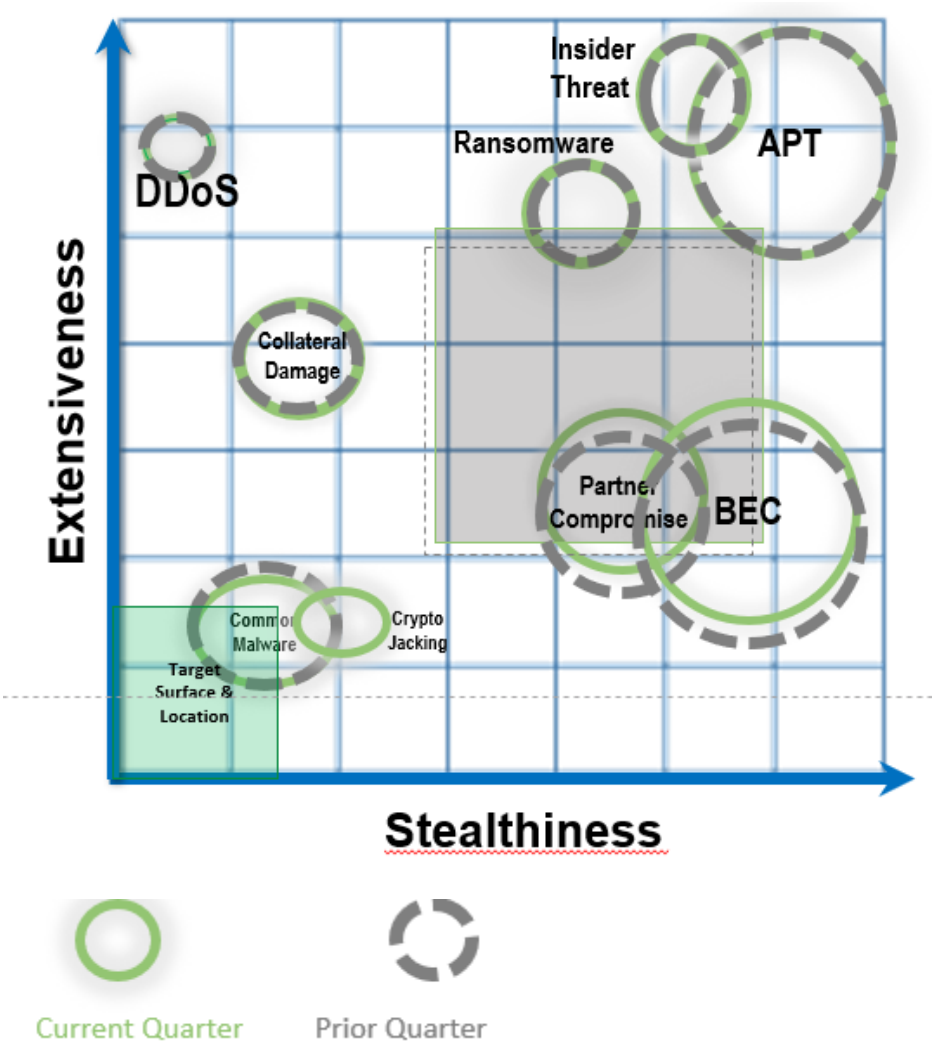
The Norsk Hydro ART (Advanced Ransomware Threat) attack of March, 2019 illustrates the risk effect of mixing diverse hosts on one network. Norsk, a major aluminum smelting company, has both 'OT' (Operating Technology), and 'IT' (Information Technology) hosts. Ovens, production lines, conveyor systems, cameras, test equipment, and other equipment that supports product design, production and testing, i.e. 'operations', are OT. Business systems, for planning, financial reporting, communications and collaboration are IT. Having these on the same network mingles, and multiples, risks. Best practice is to separate these networks. Data generally will be required to migrate between the two networks, as hosts will need to travel say between New York and Georgia, so some controlled boundary migration process is required to protect both the 'OT enclave', and the 'IT network'. One simple model is referred to as 'sheep dipping'; the practice of scanning and

cleaning files, or travelers, at a point of exchange. By enclaving hosts with similar risk profiles risk complexity is reduced. Single governance regimens can then be applied across a *bounded network*, be it biological or electronic.

In a cyber network, risks facing individual machines vary. A machine at the network perimeter, facing the internet for example, is exposed directly to certain risks that other machines may be exposed to less directly, or not at all.

Effective risk management decision making in both domains requires a defined and quantified risk tolerance standard, and its uniform application within the boundaries of a given network. There may be different effective strategies for different types of networks, however these must each then be put into operational governance **within**, and **not across**, network boundaries. This implies controls at the network boundary, be that a border-crossing, an airport arrivals hall, or a network's firewall. The menu of risk management strategies, sometimes referred to as the 'four 'T's' (Tolerate, Treat, Transfer, Terminate) are used to compose an appropriate strategy for a given network. Within the network boundary, there must be one standard risk-appetite and network policy.

To describe a cyber risk environment, and to quantify the likelihood and expected impact of various cyber threats, a chart such as this one may be used:



The risk surface, or magnitude, of each threat type is reflected by the size of each oval, proportional to the likelihood of a successful attack this quarter, and the oval's position indicates the expected impact, with the upper right of the chart the most impactful. The sum of the areas, and positions, of the individual ovals is aggregated in the central grey square, and this is the quantified cyber risk exposure of the network. In this example, the aggregate likelihood of a successful attack this quarter is portrayed as 18%. The green square at the lower left represents the target risk surface, an expression of the organization's risk appetite, which in this example is 5%. Trends are illustrated by the delta between the green and grey ovals. The objective of strategy in this instance is to apply defensive resources such that the grey square migrates towards and eventually becomes identical to the green one.

Each quarter, the size and position of the threats can be recalculated based on recently measured threat density trends, changes in the defense posture, and recent outcomes. Comparing Q2 of 2020

to Q4 of 2019 for example, the vast increase in remote workers introduces additional risks in several categories. Some of these workers may require split tunneling. Some may be using personally owned devices. Their home network may be less defended than the office network. Threat actors may be more active, leveraging the pandemic's headlines for phishing attacks. And, in this time period a novel and severe Windows vulnerability has been discovered, with proof-of-concept code made available.

Stealthiness in a cyber-attack is the ability to remain undetected following initial compromise. In a pandemic, the same attribute relates to incubation period prior to symptom expression, and ability to transmit infection while asymptomatic. In both situations, as stealthiness increases, complexity of defense increases as well.

At this date (April 28, 2020) the world is at elevated risk for a major cyber outbreak along the lines of 2017's WannaCry and NotPetya. Once again there is a widespread wormable Windows vulnerability based on 'SMB' (Server Message Block, this time v3), known formally as CVE-2020-0796. And, at this time, due to wide-spread home working, cyber risk exposure is severe. This arises from less defended home networks, increased attack activity, and difficulty disseminating the large patch (~350 Mbyte) for SMB 3.1.1.

Cyber defenders need to know the distribution of immunity, just as their biological counterparts would. This information, the equivalent of a serum test assay, is knowable thru 'asset inventory'.

Which of your home-working clients are patched for CVE-2020-0796? If you had this information available, you could implement meaningful and effective risk-based decisions; i.e. clean execution of sound strategy, akin to assigning Covid-immune health-care workers to Covid-specialist hospitals.

March 21, 2008; Walter Wagner and Luis Sancho file suit in Federal District Court in Hawaii, seeking to prevent CERN, the European Center for Nuclear Research, in Geneva, Switzerland from initiating operations on its Super Conducting Supercollider. They fear the particle collisions will lead to an uncontrolled chain reaction that will produce 'strangelets', that will reduce the Earth to a dead lump of 'strange matter'. They fear cataclysm via high-energy physics.

Sidebar 3

In November 2019 there was no immunity available anywhere on Earth against either SARS-CoV-2 (the virus that causes Covid-19, or 'Corona Virus Induced Disease 2019), nor against exploits of CVE-2020-0796 (or Common Vulnerability Exposure, 2020, serialized number 0796). They are 'novel viruses' and 'zero-day exploits' respectively.

As public health teams met urgently, planning for containment of Covid, cyber security teams were working on their preparations as well.

Today there do exist antibodies for immunity against the former, and patch code for immunity to the latter. However, clean execution of sound strategy in both cases, to effectively deploy existing defensive assets, is hampered by practitioners' lack of actionable information.

Consider the following narrative:

"The trouble started in Asia. That is where the first infections appeared. They moved from host to host with astounding speed and ferocity, creating injury, disruption, and panic, in their wake. Soon, contagion had moved to Southern Europe, establishing new hot spots, growing and spreading, in short order to over 100 countries with victims numbering in the tens of thousands. North and South America, Australia, and indeed most continents were affected by contagion in due course.

Communities were disrupted as the damage spread beyond its native domain. Many industries were impacted, with transportation hard hit and health care delivery severely stressed. The economic losses that quickly ensued were so large they were measurable as a fraction of global GDP!

As technical experts analyzed the outbreak, it became clear this pathogen was driven by a new variant of an existing family of viruses. This variant had not been seen in the wild before, and there was no herd immunity. Still, some hosts suffered massive injury while others seemed to partially or even fully resist the infection and onward transmission.

Some of the professionals whose job it had been to plan for, prevent, and mitigate such massive outbreaks had failed to act timely and effectively enough to stem the tide in their communities, although good fortune did seem to intervene to prevent the worst. It was claimed that malicious individuals and governments as well as incompetent ones, played roles in the unfolding disaster. Soon it became clear that matters of hygiene among the victim populations also played a role in governing the spread of contagion.

Companies with specialty knowledge took unprecedented measures to counter the outbreak, and authorities put emergency procedures into effect."

Some readers may interpret the above narrative as describing the spread of Covid-19, and they are not wrong. However, the same narrative also describes the WannaCry(pt) computer virus outbreak of Friday, May 12, 2017.

Distinctions:

A critical contextual distinction between biological outbreaks and electronic ones is that the former injures or kills humans directly. Humans, carbon-hosts, are the direct target of RNA coded pathogens such as SARS-CoV-2.

However cyber pathogens, or malware, while directly targeting silicon-hosts, can injure and kill humans as well, indirectly. Attacks on critical infrastructure such as air traffic control systems, dams, electricity grids, water supplies, etc., can cause mass-casualties. Hacking of vehicles, medical devices, or home networks, could lead to localized injuries in people.

The main technical distinction between these two network compromises lies in the meaning of '**astounding speed**' in the narrative above. Coronavirus infected its first 100,000 humans over a period of approximately 10 weeks, while WannaCry infected 300,000 computers in 9 hours. These vastly different time-constants drive different implementation requirements, even for parallel strategies. For a company of 11,000 employees, with 20,000 computers, if one assumes the company's employees and computers are equally at risk as those globally, the point at which the company statistically would have expected 3 WannaCry-infected computers, with 95% likelihood of at least one, was at 9 hours into the outbreak. This company's expectation of 3 Covid-infected employees arrived fourteen weeks into the outbreak.

In pandemic defense, *containment* is employed at the tails; at the outset and near the end, when the numbers of cases are low enough to allow for each case to be followed up on individually with detection, tracing, and isolation.

During the peak of a pandemic, case tracking (and health-care systems) are overwhelmed and not able to function effectively, and to minimize this a *mitigation* strategy is adopted. In an electronic outbreak, such as WannaCry, the spread of contagion is so rapid that containment procedures would not have been possible at any point during the outbreak. The same forensic work, identifying the chain of contagion or 'case tracking', is required, however, not to slow the spread of the outbreak. This work is done afterwards as part of post-mortem and attribution efforts.

For cyber professionals this is generally accomplished through review of logs, forensically, *after* the spread has completed. For certain longer duration attack chains, such as APT, Insider Threat, and ART, however, containment could be directly employed. These attack chains are typically not 'outbreaks'. Outbreak refers to *rapid* and uncontrolled chain reaction.

Both types of networks are comprised of interconnected hosts. Humans are direct participant nodes in cyber networks, in that their actions may be elements of an attack chain. Social engineering, manipulation of the human node, often plays a significant role in cyber attack strategy. Computers, while possibly useful in designing bio-warfare pathogens, or treatments, are generally not a direct participant node in biological networks.

Key variables driving contagion spread characteristics in both kinds of networks include degree of connectedness and preponderance of host immunity. However, time constants, both for latency and speed of transmission, are generally orders of magnitude swifter electronically.

The speed with which the outbreaks can be *controlled* is also distinct; WannaCry was fortuitously halted, at least temporarily, in its tracks when a researcher discovered and executed a 'kill switch'.

Covid-19 is likely to subside gradually, mirroring its relatively gradual rise. The different timeframes for electronic and biological network compromise arise from differing speeds of host-connections; the former being electronic at nearly the speed of light, the latter being bio-chemical and mechanical.

Incubation and latency periods are also likely to be shorter in electronic networks, than in biological ones, with possible exception for 'persistent' threat types such as APT (Advanced Persistent Threat), and ART (Advanced Ransomware Threat).

However, primarily for highly targeted threats such as APT, Insider Threat, and Advanced Ransomware Threat, cyber-attack strategies are generally crafted, not emergent. In these attack chains there may be enough time to employ a containment operational defense strategy at the head and tail of the attack chain.

Interactions

Some attack vectors, and defensive strategies and tactics, applied to biological networks and electronic ones are analogous. And the advent of an outbreak in either domain can lead to outbreaks in the other.

Outbreaks of biological viruses bring new and elevated cyber risks, and cyber crises feed biological risks. These two information-based domains have become inter-twined with overlapping risk surfaces. Principles of epidemiology can be effectively applied by cyber security professionals, with some adaptations required, and vice versa. Analogous tools such as health insurance and cyber risks insurance have emerged; travel bans and firewalls: social distancing and port closures: vaccination and patching.

When battling APT, defenders have learned through experience they must first be able to ***keep them out***, *before* ***kicking them out***. This mantra is counter intuitive. Many bad cyber-crisis headlines have originated from approaching the problem in the opposite way. Our instinct is to kick the attackers out immediately. However, this will inevitably lead to a 'whack-a-mole' ('whack-a-hack') situation, as the attacker easily reenters through back doors.

This leads quickly to exhaustion of the defending resource, equivalent to overloading of the health care system in a pandemic. Cyber defenders encountering an entrenched APT compromise will need to 'flatten the curve', with tactics designed to minimize losses such as manually watching the firewall 24 x 7 to prevent large file exfiltration, while slowly building up foundational defensive capabilities: monitoring, patching, enclaving. Only once this is done can intruders be effectively evicted, i.e. the network becomes cured.

Boundary defense is implemented in part in network enclaves, with movement of hosts between enclaved areas requiring special hygiene measures, such as 'sheep-dipping'. This principle, adapted from animal husbandry, establishes hygienic boundaries, and dis-infection procedures required for any host or file crossing the enclave boundary. A parallel requirement is evident in travel bans and controls employed in Covid-19 response. When deciding between local, regional, or national re-opening strategies following lockdown, this principle translates directly: *Whatever the definition of the public health area, the policy must be uniform within that network boundary.* If Northeastern states, for

example, adopt a re-opening strategy aligned to unique factors at play there, while Mid-Western states adopt a different one, then travel of hosts across this inter-network boundary must be controlled. Containment at the boundary allows for different defense regimens in adjoining networks.

Offense and Defense:

Consider that through natural selection, prey species have evolved a set of similar visual adaptations, distinct from predator species. The goat's eye's, pictured below, have a horizontal pupil, while the alligator, a predator animal, has a vertical pupil. This adaptation arises from the most fundamental of *defensive* strategy requirements, that of scanning and monitoring, in biological terms 'testing', or surveying the landscape for threats. The foundational strategy of *attack* is the opposite, *focus*.

The entire visual systems of evolved organisms, not only the pupils, are tailored for their primary niche. Humans, and other species that occupy both predator and prey niches, have evolved a hybrid system, with features including round pupils.

Defenders of public health, and computer networks, are defenders of *prey*. To the cyber defender, this fundamental mandate is expressed with *monitoring* at network boundaries, internal and external. To the public health professional, it is expressed through surveillance and assay *testing*.

When there is uncontrolled, rapidly spreading contagion, how would a cyber security professional implement a defensive strategy analogous to containment and mitigation in a pandemic? Having such a capability would have provided a powerful defense, for example, during WannaCry.

This is in part the concept of *Defcon Orange*; a temporary establishment of a firm boundary at the network's external perimeter, similar to a travel ban.

… Reacting Quickly to Outbreaks

- When environmental outbreaks are detected (for example; WannaCry, NotPetya)
- Odds of infection with 20,000 nodes, on 300,000 infections of 2B on the internet: (expected infection of 3 machines with a ransomworm)

- Temporarily quarantining inbound internet email
- Stage for temporarily disconnecting WAN segments
- Enhanced backup
- Push IOCs, Patches, Reboots
- Stage for temporarily disconnecting internet Ingress & Egress

… Containing Collateral Damage Risk

- When the threat has entered the WAN
- Quarantine inbound and outbound internet and internal email
- Temporarily disconnect WAN segments

- Implement alternative communications processes
- Temporarily disconnect internet Ingress and Egress
- Elevate all blocking tools to High Enforcement (panic button)
- Power off non protected servers
- Power off legacy systems

Defcon Red carries the concept a level deeper, it is a social-distancing defense.

These measures correspond to shut down of the national borders (Orange), and regional, local, even house-by-house level borders (Red) in a pandemic; social distancing. Developed in response to WannaCry and NotPetya, these measures provide options for swift and effective cyber risk mitigation during an outbreak.

WannaCry appeared to be an untargeted ransomware campaign. NotPetya appeared to be a targeted cyber warfare campaign. However, both of these campaigns' main impacts were the opposite. In WannaCry, ~ 999 out of each 1,000 victims did not pay a ransom. In NotPetya, a similar proportion of the damage caused was collateral; i.e. not in the targeted entity of Ukraine.

Development of Defcon Orange and Red capabilities was an appropriate response for organizations, given the speed with which each of these outbreaks spread across the internet.

However, homeworking during a pandemic fundamentally impacts the functioning of Defcon Orange and Red.

A large fraction of an entity's machines may be off site, off the LAN, and outside the perimeter of both Orange and Red, during a pandemic response. The fundamental strategy behind the Defcon responses is similar to a tortoise closing its shell … adopting a temporary defensive posture to wait out a brief dangerous period. If half the tortoise were outside its shell when the danger arose, the strategy would not be as effective.

Further, in a pandemic response world, recovery from a WannaCry II type of outbreak would be prolonged, as machines would be difficult to remediate remotely. And, erecting a barrier between the office and the internet does nothing to protect a worker on a lesser defended home network.

Adaptations to these Defcon procedures will therefore need to include deflation of VPN tunnels, since it is likely the first compromises on the network will be taking place in employees' homes. However, IT staff will need to remain connected to fight the contagion, and they, too, are at home. So, a separate VPN apparatus needs to be established and outside the Defcon protocols.

Friday May 12th, 2017; WannaCry ransomware campaign erupted globally, infecting 300k computers in 150 countries. Affected users' screens displayed the $USD300 Bitcoin demand below.

The attack was formally attributed by several nations to North Korean actors. A kill-switch, apparently included unintentionally, was fortuitously found and activated sparing many millions of vulnerable hosts. Cataclysm was narrowly avoided.

Sidebar 4

The same tactics employed to control Covid-19 spread may be considered for application in digital networks. Information on the susceptibility of hosts by category, for example older people and people with diabetes or high blood pressure, applies to computer hosts as well. Only certain versions of Windows 10 are susceptible to SMB3.1.1 exploits. Do you have an inventory of these machines, and their locations? Certain users are more phish-prone. Do you have a phish-testing and training program, and do you have a risk score for each user? Could you choose to disallow split tunneling, or use of personally owned equipment, for a user that has a legitimate need but a higher risk score?

Prior to the outbreak, have you considered and decided on appropriate levels of reserves? Hospitals manage surge ICU beds, ventilators, and PPE. Have you considered your available stocks of laptops, mobile devices, video conferencing, and surge VPN bandwidth?

Have you defined in advance what privacy 'rights' are reserved, in terms of potential user tracking, alerting, and posting? Do you have the right to scan the user's home network for security vulnerabilities, if you are asking her to work from home?

Have you established procedures to quickly vet new information in a crisis? Should masks be worn by the general public? Is Zoom safe to use for enterprise home-working? As new information arises, it must be swiftly ingested, and any tactical or strategic changes arising must be deployed. Mechanisms for collaboration, and secondary channels for communication, are required to enable this.

At the initial rise of the outbreak, and the tail, can you apply the principles of case management: testing, identification, quarantine?

This table provides a list of potentially analogous terms in the two domains:

Biological Network Term	Electronic Network Term
Antibody	IOC/Signature
Containment	Segmentation
Epidemic	Outbreak
Flattening the curve	Defcon Red, Defcon Orange
Herd Immunity	Herd Immunity
Isolation	Air Gapping
Mitigation	Mitigation
Mutation	Variant
Novel Virus	Zero-day Exploit
Pathogen	Malware
Patient Zero	Initial Compromise
Personal Protective Eqpt.	End point defense
Quarantine	Enclaving/Quarantining
Social Distancing	Closing Ports
Testing	Monitoring
Vaccine	Patch

TABLE 1: ANALOGOUS TERMS

Adaptations need to be added to Defcon playbooks, each reflecting new risk profiles arising from pandemic-response-driven network changes. Patching for SMB3.1.1 for example may be optimized, over skinny VPN pipes by lengthening VPN timeout constraints and pushing patches overnight. This strategy parallels one to vaccinate health-care workers first.

Home networks can be scanned for vulnerabilities. Split tunneling can be disabled for workers whose jobs don't require it, akin to providing N95 masks to health-care workers and cloth masks to civilians.

Risk tolerance levels can be reduced. For example, by blocking an entire partner domain when only a single email-box might be compromised, and blocking non-malicious spammers, to lower the noise floor, and assigning online cyber security training for users following small errors. Shifting towards the 'whitelist' or 'allowlist' side of the spectrum, for example by blocking all email from newly registered domains, is prudent when risks are elevated. This tactic might be unacceptable to a fast-growing organization in normal times. However, it makes sense when hunkering down amid 100,000 newly registered malicious domains, with large numbers of workers out of range of some of the company's network defenses. These shifts are akin to reducing allowed social group sizes, say from fifty people, to ten, to two.

Being able to load IOCs to end points substantially reduces this added risk from remote working. If your organization maintains an IOC library, and is able to deploy these IOCs to appropriate tools,

this becomes a connected defensive structure which can adapt to home working. This capability reduces the risk-penalty for home working substantially. It is akin to a vaccination.

Additional user training is critical. There will be a temptation to pause phish-click type training and postpone face-to-face cyber security training, to avoid overloading employees already frazzled trying to meet quarterly targets while working remotely.

However, the opposite must be done. Phish training must be supplemented with Covid-themed templates, and tolerance levels for employee performance made tougher, rather than relaxed. Safe homeworking training should be assigned to anyone logging in via VPN. This is parallel to public-health messaging.

False positives are likely to arise as the network profile quickly changes. Users may move a lot of files around in preparation for home working, possibly triggering false alarms for ransomware activity. Desktop machines moved to an employee's home may disrupt DNS patterns and lead to DNS DDoS false positives. Local IT teams may elevate users' privileges to allow them to load SW once they get home, further increasing risks. CIRT teams will need to anticipate these kinds of events.

Should a cyber outbreak occur during the lock-down period, incident response would be more complex. The essential first step is having a secondary method of communication available for the CIRT team.

In Conclusion:

Cataclysm arises when a previously stable network structure is ravaged by uncontrolled chain reactions. Analog cataclysms, arising from atomic weapons, Ice Nine, or black holes, could still arise. However, we've come face to face with digital cataclysm more than once recently and seen how fragile our digital internet-based nervous system is. Digital networks promise amazing societal benefits, such as finding cures for diseases by applying analytics to electronic medical records and managing traffic in congested cities. However, these benefits cannot be realized unless the cyber security problem is solved. The fundamental advantage of digital design vs. analog, is design re-use. Digital programs and data are easily *reproduced*. Replication is in its nature, as it is in SARS-CoV-2's.

Uncontrolled replication is today's most prominent cataclysm risk, be it a binary-coded ransom-worm, or a quad-coded RNA virus outbreak.

Epidemiologists and health-care providers, and cyber-security professionals and incident responders, share closely related missions, and toolboxes.

Dr. Corey Hirsch, CISM, serves as CISO at Teledyne Technologies, and is a graduate of the FBI's CISO Academy. He teaches cyber security on Columbia University's Masters programs in Enterprise Risk Management, and Technology Management. These views are the author's, and do not represent Teledyne Technologies' or Columbia University's.