IT'S THE CYBERCRIME AND ITS SPONSORS (NOT MY CYBER-SECURITY), STUPID

David N. Lawrence, Frances Townsend, Tim Murphy, Jeff Castelli, Daniel Garrie, John Squires, Eric Herschmann, Serina Vash and Matthew Lawrence [*] [†]

There is a mysterious cycle in human events. To some generations much is given. Of other generations much is expected. This generation of Americans has a rendezvous

---

[*] David N. Lawrence is the founder and chief collaborative officer of the Risk Assistance Network+Exchange (RANE), and was formerly associate general counsel and managing director at Goldman Sachs. Previously, he served in various senior positions with the United States Attorney's Office, (S.D.N.Y.). Frances Townsend is executive vice president of MacAndrews & Forbes and National Security Analyst for CBS; and was formerly Homeland Security advisor to President George W. Bush. Tim Murphy is President of Thomson Reuters Special Services, where he leads public-private sector efforts to address cyber and a wide range of law enforcement and national security issues. Formerly, he served as Deputy Director of the FBI. Jeff Castelli is the executive vice president, Federal, at the cybersecurity company, Endgame, where he leads their efforts with government agencies. He served for 30 years at the highest levels of the U.S. government on national security matters, serving abroad for more than 17 years. Daniel Garrie is a neutrals with JAMS, Editor-in-Chief of the Journal of Law and Cyber Warfare, and Executive Managing Partner of Law and Forensics. John Squires is a senior partner at the law firm of Dilworth Paxson, specializing in intellectual property and technology law, and served as chief IP counsel for Goldman Sachs. Eric D. Herschmann is a partner at Kasowitz, Benson, Torres & Friedman, LLP, where he specializes in complex regulatory, litigation and commercial matters. Previously, he served as Vice Chairman of the Board, President, Chief Operating Officer and General Counsel of the Southern Union Company, and as an Assistant District Attorney in Manhattan. Serina Vash, is the Executive Director of the NYU Program on Corporate Compliance and Enforcement; and is a former senior prosecutor with the United States Attorney's Office in New Jersey. Matthew H. Lawrence attends Fordham University Law School, is a graduate of Brown University (Concentration in History), and previously worked at Perkins Coie, LLP. He is involved in researching and writing on a wide range of legal, commercial, and social issues.

[†] Contributing Authors: Adam B. Frankel is the General Counsel of the investment bank, Evercore Partners, and is a member of the Council on Foreign Relations. Joel Krauss is the Global Director of Security for WeWorks, and was formerly the Director of Safety and Security for the International Rescue Committee; for over 20 years, he served in a variety of senior security positions for the US government. Adam Robinson is the CEO of Robinson Global Strategies, and is the former founder of the Princeton Review education service. Elad Yoran is Executive Chairman of KoolSpan, CEO of SGP, and an advisor at the Army Cyber Institute. He has advised a number of U.S. government agencies. Previously, Elad served as a US Army officer and is a graduate of the Wharton School and West Point.

Disclaimer: The views expressed by the authors are entirely their own and should not be attributed to any of the institutions with which they are—or have been—affiliated.

with its digital destiny. In this world of ours, there are some people who have sold their heritage of freedom for the illusion of a living. They have yielded their democracy. The preservation of our democracy is far from a given. Every generation has the obligation to defend it—for themselves and for future generations. It should not take another day of infamy—a digital Pearl Harbor—to hear this calling.[1]

(Franklin Delano Roosevelt, only slightly updated for the digital age.)

ABSTRACT

"It's the economy, stupid", was the simple message that political strategist, James Carville crafted in 1992 to successfully communicate the priorities of President Clinton's first campaign. The authors argue that we are long overdue in delivering a similarly simple message about protecting our nation and our people in an increasingly interconnected world:

> *It's the cybercrime and its sponsors—not your cybersecurity—stupid. And we have a plan to address it together for everyone's benefit.*

The authors note that the defense of our nation against all threats, foreign and domestic, has always relied upon cooperation and assistance between our citizens and government. Neither sector has ever been asked, nor is able, to go it alone. Cybersecurity can be no exception.

They make the case for going "back to the future" to find the proven pathways forward for greater security. In

[1] *82 - Acceptance Speech for the Renomination for the Presidency, Philadelphia, Pa.*, AMER. PRES. PROJECT, http://www.presidency.ucsb.edu/ws/?pid=15314.

doing so, they draw inspiration from: 1) The Constitution (Article II)—the requirement to share the information that is "necessary and expedient" to understand the State of the (Digital) Union, 2) The Declaration of Independence (Interdependence)—to explain why we can no longer adhere to our existing forms of (cyber) governance, and 3) Ben Franklin—for his "open-source" products and networks to manage the known, but unpredictable, cyber-risks that affect us all.

As the authors point out, our Founding Fathers understood that words and ideas based on empathy, utility and simplicity were essential to bring people together to solve their common and most complex problems. Their guiding principles about the actions that can protect and promote the public good have proven timeless in sustaining our "experimental" nation. For good reason, the DNA of their thinking survives within many of today's most innovative public and private sector achievements. We should now look to these analog approaches to mitigate our digital exposures.

Time is of the essence.

An Introduction

In 1972, spies working for the President of the United States broke into the Watergate headquarters of the Democratic Party with black bags and eavesdropping equipment. Their goal was to steal confidential information and a Presidential election. They were discovered in the act by an alert night watchman. The police were called, the plot was thwarted, hearings were held, the co-conspirators were prosecuted, and a sitting President resigned in disgrace. Aptly named the "White House Plumbers", one of this gang's earlier missions had been to stop the *leaks* of the

Pentagon Papers by stealing and publicizing the psychiatric records of the source, Daniel Ellsberg.

45 years later, spies accused, by some, of working for the President of Russia—operating safely and anonymously from distant shores—allegedly used far more sophisticated methods and means to steal and leak the communications of the Democratic National Committee (DNC), hack into other national and state groups, and disseminate "false" news to the American public. While still the subject of ongoing investigations, their alleged goals include: destroy a candidate's credibility, undermine confidence in our democracy, and produce the "Divided States of America". This time, there was no security guard to detect the break-in and no police to respond. The thefts and leaks went on for many months, hearings were held but no officials resigned, and the conspirators remain unnamed, unindicted and at large—at least for now. Ironically self-proclaimed as "Cozy Bear" and "Fancy Bear", it was not the first mission credited to these two anonymous groups, and it is unlikely to be the last of their warm and cuddly acts. Evidence suggests an even broader and ongoing scope to this plot.

Amidst growing evidence of Russia's possible involvement in the United Kingdom's "Brexit" vote to leave the European Union (EU) and Ukrainian elections, Western intelligence agencies have openly warned of broader Russian efforts to influence upcoming European elections and destabilize the EU.

This "mysterious" cycle of cyber events surrounding our recent elections may not have been entirely expected, but it was foretold. In dropping a web of hacks, leaks and disinformation upon our democratic process, these assaults logically and seamlessly joined a string-theory continuum of escalating cyber "wake-up calls" that are neither "one-off" events, coincidental, nor the work of just a few bad actors in "hoodies".

Ominously, the 1984 Presidential race warned about the "bear" and its intentions, even before its "cubs" (and Panda neighbors) went online:

> *"There is a bear in the woods. For some people, the bear is easy to see. Others don't see it at all. Some people say the bear is tame. Others say it's vicious and dangerous. Since no one can really be sure who's right, isn't it smart to be as strong as the bear? If there is a bear."*[2]

Lest a full refresher course be needed that there are "bears" in our digital woods—and that it would be smart to be as strong as these "bears"—the last several years have yielded among these encounters: the worst hackings of government systems and personnel records in history (federal and state), massive "insider" leaks of national security data, the theft and leaks of billions of consumer records and personal communications, losing hundreds of millions of dollars from financial institutions and money- transfer systems, systemic breaches of our military and defense commands, penetrations of essential infrastructure controls (police, power grids, communications, water and transportation), industry-wide lootings of competitive secrets and intellectual property (IP), hijackings of company systems and communications for extortion and ransom, breaches of law firms' client information, the thefts of hospital and insurance records, burglaries of universities for their research IP and records, the hacks of scientific climate data ("Climategate"), the probing of voter registration and voting machines, and the take-down of significant swaths of the Internet by commandeering hundreds of thousands of

[2] *Bear*, MUS. OF MOVING IMAGE, http://www.livingroomcandidate.org/commercials/1984/bear

household devices— to name just a few of the events made public.

More recently, the U.S. Energy Department issued a public warning that the nation's entire power system—including nuclear—"faces imminent danger" from cyberattacks, which are growing more frequent and sophisticated.[3]

The cyber age has even reinvented the old Soviet art of "Kompromat" (compromise), giving the geopolitical playbook of blackmail and leverage new scale and reach. Who needs the trouble and expense of bugging a hotel room and recruiting a seductress, when nothing is easier or proves more authentic than hacking and releasing the embarrassing data of someone's own words, actions, afflictions, and preferences?

Within a media market where "eyeballs" are prized more than Pulitzers—delivering the advertising revenue that "keeps the lights on"—just the hint of a hack is more than enough for "virtually" believable news to go viral.

As Mark Twain would have observed about our current state of affairs: *If history does not repeat itself exactly, it sure as hell rhymes online.*

Run DNC. Run all.

In the aftermath of our reported "hacked elections", we once again heard a call to action. Senior officials found their footing and stayed on message. We will take any and all necessary action to defend the integrity of our democracy. We have a wide range of options: from sanctions to

[3] Ari Natter & Mark Chediak, *U.S. Grid in 'Imminent Danger' From Cyber-Attack, Study Says*, BLOOMBERG: MARKETS (Jan. 6, 2017), http://centeronnationalsecurity.us11.list-manage.com/track/click?u=85c3b78d73a97cc0aeb73a203&id=5f21461979&e=26abc4feca.

indictments to hacking-back to launching a crippling cyber counter-attack. We will respond at a time and place of our choosing—and under the circumstances that will have the greatest impact. Some of our actions may become public, some may not. Some may be so covert, the targets may not even realize they have been hit.

In tandem, President Obama also ordered American intelligence agencies to produce a full report (in classified and declassified forms) on Russian efforts to influence the elections, to include a list of "lessons learned". Bi-partisan leaders meanwhile convened a separate Congressional investigation to understand Russia's "multifaceted campaign" (as well as to learn about the activities of other states, such as China, Iran and North Korea)—and how we should respond. Then President-elect Trump weighed in with a promise to convene a "Cyber Review Team" of military, law enforcement, and private sector personnel to enhance national strategies for training, threat detection, and offensive and defensive deterrence capabilities against foreign hackers.[4]

Left for another day was any real analysis or debate about our own cyber efforts to influence the affairs of other nations—and whether, in reality, we have become the unsuspecting audience-participants in a digital revival of *Mad Magazine's Spy vs. Spy*.

After these events and so much more, do we still believe that the information super-highway only paves-over established business models and not entire nations?

---

[4] After assuming office, President Trump immediately considered a draft executive order on cybersecurity. *See Read the Trump administration's draft of the executive order on cybersecurity*, WASHINGTON POST, https://apps.washingtonpost.com/g/documents/world/read-the-trump-administrations-draft-of-the-executive-order-on-cybersecurity/2306/.

Admittedly, every past "wake-up-call" seems to have come with its own snooze button, allowing us to drift off until the next event. As President Obama acknowledged following the 2016 elections, we "underestimated the degree to which, in this new information age, it is possible for misinformation, cyber-hacking and so forth, to have an impact on our open societies."

There are 3 "W's" at the heart of our cyber crisis and our current struggles for solutions:

- Why we are where we are
- Where we must go
- What we must do to get there

Answers are needed. We have found them before.

We know from past events that our best decisions seldom come during the flashpoint of a crisis—when politics and emotions can run white-hot. Within this moment of relative calm, we can provide foresight, not hindsight; a biopsy, not an autopsy; a blueprint, not a *Code Blue*. While completely eliminating our cyber risks may be impossible, we can certainly achieve far more effective mitigation, deterrence, and resiliency (anti-fragility).

Fortunately, there is a pathway forward. We just need to go "back to the future" for the *analog* answers to our digital exposures.

To do so, we need look no further than our Founding Fathers and the ideas that formed "a more perfect union" (not a perfect one) imbued with the agility to correct over time. Their guiding principles about the words and actions that can protect and promote the public good have proven timeless in sustaining this "experimental" nation. They discovered that empathy, utility and simplicity were among the ingredients that brought people together to solve their common problems. Whether knowingly or unknowingly,

intentionally or not, later policy-makers and entrepreneurs have inserted that same DNA into many of today's most valuable public and private sector achievements.[5] It is now time to link these ideas to address our cyber crisis. Time, however, is of the essence.

For the framework of our discussion, we thus shamelessly borrow from: 1) *The Constitution (Article II)*—the requirement to share the information that is "necessary and expedient" to understand the *State of the (Digital) Union*, 2) *The Declaration of Independence (Interdependence)*—to explain why we can no longer adhere to our existing forms of (cyber) governance, and 3) Ben Franklin—for his "open-source" products and networks to manage the known, but unpredictable, cyber-risks that affect us all.

We also begin with a reminder that cyber is not a case of technological first impression. There is precedent that is directly on point.

On October 4, 1957, the Soviet Union successfully launched the world's first artificial satellite into orbit. Sputnik was about the size of a beach ball, weighed only 184 pounds, and took about 98 minutes to orbit the Earth. It was followed a month later by Sputnik II, which carried a heavier payload, and a dog. Fewer than four years later, Russian cosmonaut Yuri Gagarin orbited the earth, becoming the first human in space.

As a technical achievement, the Sputnik satellites drew the world's attention and caught America off-guard. Visible to the naked eye as they sped through the night sky, these satellites marked the start of the space age and a new frontier in the race between the America and the U.S.S.R. to

---

[5] *See e.g., The Key Leadership Skill that Steve Jobs and Ben Franklin Share*, KNOWLEDGE@WHARTON (Oct. 7, 2016), http://knowledge.wharton.upenn.edu/article/steve-jobs-benjamin-franklin-common/.

determine the future course of history on Earth.[6] When the Soviets orbited the Earth in April 1961, it was far more than an act of exploratory achievement. It became the very embodiment of the Soviet Union's military might and ambition, stoking legitimate fears about Soviet nuclear superiority and the potential of inter-continental ballistic missiles raining down from space.

After all, Soviet Premier Nikita Khrushchev had already promised the West: "My vas pokhoronim,"—"We will bury you".[7]

In May 1961—just one month following the Soviet's successful orbital flight— President Kennedy reassured a panicked nation in an address before a joint session of Congress. His words clearly and urgently defined the issue, what was at stake, and the need for a national commitment to do more than catch-up to our present exposures. If we were to secure our future, we needed to move ahead of present events with speed, agility, and a grand vision—unafraid of our inevitable failures being in full view of the world. We needed to be the first to reach the moon.

President Kennedy's speech should be read in its entirety, not simply for its profile in courage at a moment in time, but because it perfectly transposes to our present race for digital security.[8]

(Of significant note, our national space effort yielded more than a moon landing—it produced many of the brilliant minds and ideas responsible for today's digital machines and neural networks.)

---

[6] *Sputnik and The Dawn of the Space Age*, NASA (Oct. 10, 2017), https://history.nasa.gov/sputnik/.
[7] *Foreign News: We Will Bury You!*, TIME (Nov. 26, 1956), http://content.time.com/time/magazine/article/0,9171,867329,00.html.
[8] *Excerpt from the 'Special Message to the Congress on Urgent National Needs'*, NASA (May 24, 2004), https://www.nasa.gov/vision/space/features/jfk_speech_text.html.

For the convenience of our readers, we have excerpted some of the relevant passages of President Kennedy's speech, and joined the word "cyber" to "space" to address our present "Sputnik" moment:

> Finally, if we are to win the battle that is now going on around the world between freedom and tyranny, the dramatic achievements in [cyber]space should have made clear to us all, the impact of this adventure on the minds of men everywhere, who are attempting to make a determination of which road they should take. We have examined where we are strong and where we are not, where we may succeed and where we may not. Now it is time to take longer strides—time for a great new American enterprise—time for this nation to take a clearly leading role in [cyber]space…which in many ways may hold the key to our future on earth.
>
> I believe we possess all the resources and talents necessary. But the facts of the matter are that we have never made the national decisions or marshaled the national resources required for such leadership. We have never specified long-range goals on an urgent time schedule, or managed our resources and our time so as to insure their fulfillment.
>
> This decision demands a major national commitment of scientific and technical manpower, materiel and facilities, and the possibility of their diversion from other important activities where they are already thinly spread. It means a degree of dedication, organization and discipline which have not always characterized our research and development efforts. It means we cannot afford undue work stoppages, inflated costs of material or talent, wasteful interagency rivalries, or a high turnover of key personnel.
>
> New objectives and new money cannot solve these problems. They could in fact,

> aggravate them further-unless every scientist, every engineer, every serviceman, every technician, contractor, and civil servant gives his personal pledge that this nation will move forward, with the full speed of freedom, in the exciting adventure of [cyber]space.[9]

Finally, a quick but fulsome disclaimer: what we have written is derivative of the thinking of many others. We do not hold ourselves out as the brightest people in the room—only to having had access to some of the rooms that held the brightest minds and having been able to listen, learn, and think.

We are committed to honoring that privilege and process—and continuing to "*lean in*" and very much *upon*.

We have also far exceeded 140 characters and thus the boundaries of today's most effective messages. Hopefully, we have justified the length of our words with some weight.

We welcome and look forward to adding your words as well.

The State of Our Digital Union—What Has Divided Us

The defense of our nation against all threats, foreign and domestic, has always relied upon a social contract of cooperation and assistance between our citizens and government. Neither sector has ever been asked, nor able, to go it alone. Cybersecurity can be no exception.

Ironically, the sources and nature of our cyber threats are neither new nor technological. The portals may have changed, but the actors and their plots remain the same.[10]

---

[9] *Id.*

[10] Cy Vance Jr., CHARLIE ROSE (Jan. 22, 2015), https://charlierose.com/videos/25921.

Once again, our nation confronts a familiar cast of criminals, hostile states, terrorists, and "mischievists"—seeking to commit the all-too-familiar acts of theft, fraud, espionage, extortion, blackmail, sabotage, terrorism, human rights violations, disinformation, and destruction. Once more, we find ourselves in a moment and place that, *for every reason*, should be the "same as it ever was"[11]—where known threats to our collective safety and security should already have compelled and inspired us to find the ways and means to band together.

And yet, this solution has not happened—at least, not yet.

The question is why?

In February of 2016, President Obama elevated cybersecurity to the same importance as terrorism. He created, by executive order, the bipartisan Presidential Commission on Enhancing National Cybersecurity ("Commission")[12] to strengthen digital security in both the public and private sectors. Comprised of some of the "brightest minds" in technology and security from inside and outside the government, 12 commissioners[13] were mandated to develop short-term and long-term measures to protect privacy, to ensure public safety and economic and national security, and to empower Americans to take better control of their digital security."[14]

---

[11] Edgar Aldrett, *Talking Heads - "Once In A Lifetime"*, YOUTUBE, https://www.youtube.com/watch?v=I1wg1DNHbNU

[12] *Commission On Enhancing National Cybersecurity*, NAT. INST. FOR STAND. & TECH., https://www.nist.gov/cybercommission.

[13] *Commission On Enhancing National Cybersecurity: Commissioner List*, NAT. INST. FOR STAND. & TECH., https://www.nist.gov/cybercommission/commissioners.

[14] In June 2015, we had shared the idea for the formation of such a commission in an opinion piece, *see* David Lawrence et al., We Don't

The Commission released their report in December 2016, after spending the better part of a year conferring with numerous technical and policy experts, holding public hearings, and reviewing extensive materials. The experts providing input ranged from academics, scientists, and lawyers, to business leaders (finance, insurance, technology, energy, communications and infrastructure), to experts in counter-terrorism, intelligence, and consumer protection and privacy.

While the report offered a number of recommendations about what is needed to improve cybersecurity in six specific areas—infrastructure, investment, consumer education, workforce capabilities, government operations, and global digital economy—it also reached an overall conclusion subsequently summarized by one of its Commissioners:

> *"What we've been doing over the last 15 to 20 years simply isn't working, and the problem isn't going to be fixed simply by adding more money.*[15]

In the course of its work, the Commission essentially had to answer a fundamental gating question that has brought us to this crisis point. We have paraphrased it:

Need a Crisis to Act Unitedly Against Cyber Threats, KNOWLEDGE@WHARTON (Jan. 5, 2017), http://knowledge.wharton.upenn.edu/article/we-dont-need-a-crisis-to-act-unitedly-against-cyber-threats/.

[15] Tami Abdollah & Darlene Superville, *Panel Urges Better Cybersecurity to President-Elect Trump*, SCI-TECH TODAY (Dec. 5, 2016), http://www.sci-tech-today.com/news/Trump-Briefed-on-cybersecurity/story.xhtml?story_id=0110018845FY.

With so much at stake and so many smart people, why to-date has there been so little collective progress?

Relevantly, the Commission's report revealed three themes that have defined this security crisis: 1) we have lacked sufficient collaboration between and among all sectors—and, hence, meaningful coordination of the expertise and information to manage the growing threats, 2) we must move the responsibility for (or burden of) cybersecurity away from individual enterprises and citizens, and handle it at higher levels for everyone's benefit, and 3) the reason for our dilemma—why we are where we are—may have little to do with the complexities of our digital networks or our lack of knowledge and expertise. Instead, it may have everything to do with human behavior and our failure to fully leverage critical lessons about problem solving and crisis management—including the need for approaches that build trust, empathy, utility, and simplicity.

Notably, one commissioner highlighted that some senior information technology managers distrusted their own government as much as they distrusted China, widely regarded as actively hacking into companies here and abroad.

In politics as in life, words matter. So does simplicity. When tackling issues large and small, it is not merely what we say—it is what people hear. It is also whether our words and ideas have the utility to translate into solutions.

" It's the economy, stupid", was the message that political strategist James Carville crafted to direct the focus of President Clinton's successful campaign in 1992. Early on, Carville recognized the central importance of the issue, and the need to simply communicate the campaign's priority and plan to the American public.

In our policy arenas, we have learned to choose our words with purpose and care, mindful of their impact on public opinion and potential consensus building. Unity requires its own language. It is why we say "death tax" not "estate tax", "opportunity scholarships" not "vouchers", "electronic intercepts" not "eavesdropping", "affordable healthcare" not "socialized medicine", "reproductive" not "abortion" rights, "energy exploration" not "drilling", "equality of marriage" not "gay rights", "progressive" not "liberal", and "climate change" not "global warming". It explains our choice of legislative acronyms like PATRIOT[16] and JOBS[17]—and, in part, why using the word "privatize" doomed needed social security reforms. It is also why we are still debating the "correct" words for discussing the nature and sources of terrorism.

Relatedly, leading innovators have shown how market-based solutions based upon simplicity and utility—rather than upon complexity—can quickly influence and incentivize changes in our behavior. On a global basis, it explains the success of such innovations as: single-click, screen-touch, and voice computing, smart phone devices, online research and shopping, direct deposits and index investing, digital streaming, social media's organizational reach, communications in 140 characters, 3 numbers for reporting danger (911), the text alerts that mobilize a willing public, and the "*UL"* (Underwriters Laboratory) certification that for more than a hundred years has allowed consumers to trust the safety of their electrical appliances.

Modern innovators and scholars have unpacked some of our most complex problems and behaviors to understand why we do what we do—and why some solutions

---

[16] *The USA PATRIOT Act: Preserving Life and Liberty*, DEP'T OF JUSTICE, https://www.justice.gov/archive/ll/highlights.htm.

[17] *Jumpstart Our Business Startups (JOBS) Act*, SEC. & EXCHANGE COMM., https://www.sec.gov/spotlight/jobs-act.shtml.

to our problems succeed and others fail. Their fields range from economics and finance (Sunstein, Shiller, Thayer, Thaler, Taleb, Bogle), to communications and politics, (McLuhan, Schwartz, Axelrod, Luntz, Lakoff), to technology (Engelbart, Jobs, Brin, Zuckerberg, Dorsey), to business and legal (Adam Grant, Alan Siegel, Jim Collins, Philip Howard), to behavioral psychology (Milgram, Janis, Festinger, Gladwell, Atran, Vedantam).

Here are a few of the "common denominator" conclusions about what works—and, conversely, what we ignore at our peril:

- Keep ideas simple to understand and use. Problems are not inherently intractable. It is the complexity of our approaches that often keeps them so.
- Apply empathy. Stand in the shoes of those impacted. Solutions based on simplicity and utility will follow.
- Choose our words, messengers and mediums with care. They may matter to the audience as much as—if not more than—the idea itself.
- Fear the paralysis of perfection more than failure. It is the enemy of the good. Speed and agility matter. Communicate that our solutions remain a work-in-progress and will be improved upon as you learn more. Continuously show the empathy and agility to do so.
- Build in resiliency (anti-fragility) that can adapt to the unexpected.
- Heed the "gating" advice of Steve Jobs and others. Achieving simplicity is not easy. It can be harder than complex. But in the end, the results will be worth it.

Unfortunately, in confronting our cyber crisis, we have yet to apply these very lessons to effectively communicate the urgency and shared nature of our online risks—no less offer the empathy, utility, speed, and simplicity needed.

To the contrary, the daily reality of *Cyberland,* has been more akin to the fantasy trial in *Alice in Wonderland*. We have turned upside-down our successful models for mutual security and police-community relations by choosing messages and policies that:

- Label successful attacks as "security failures".
- Charge victims as criminals and hold them liable for damages.
- Allow perpetrators to remain free to reap their rewards and attack again.
- Insist (or pretend) that our people and enterprises can somehow fend off the global criminals and geopolitical sponsors behind these attacks, even when the government—with its vast expertise, resources, and intelligence capabilities—cannot protect itself.
- Turn our regulators into "beat" cops with nightsticks, who seek to lower crime rates by hitting victims over the head for knowing they were attractive, inviting the assault and then failing to fend-off their attackers.
- "Sentence first, verdict later"—presumptively blaming and shaming victims, further discouraging them from coming forward.
- Impose complex and fragmented regulations from a myriad of state and federal agencies—offering no bright-line rules or "safe harbors" for good faith compliance.
- Double tax the innocent—once for the costs of compliance, and later for any errors and omissions.

- Impose "Catch-22" disclosure requirements to punish victims when they come forward, and when they fail to do so.
- Ignore "double jeopardy" standards of fairness and closure, allowing long-term liabilities involving multiple fines, lawsuits, hearings, etc.
- Expand and even mandate by regulation the use of digital highways—even when knowing they are "unsafe at any speed".
- Require costly "check-the-box" expenditures for 10-foot high firewalls, knowing attackers can get 15-foot ladders.
- Outlaw the right to bear any (digital) arms that might hurt the source of an attack, eliminating real-world notions of self-defense and general deterrence.
- Allow a marketplace where solutions and ideas remain quarantined in silos—whether due to costs, limited production, or lack of public awareness—while we efficiently match supply with demand in so many other aspects of our lives (manufacturing, marketing, travel, employment, shopping, finance, entertainment, dating, etc.).
- Avoid debating whether parts of our government—in the name of national security—are purposely not sharing known security gaps in software and systems or the means and timing of attacks, lest they compromise their own (offensive and defensive) cyber activities and capabilities.
- Inform our citizens and their enterprises: unfortunately, your government cannot protect you anytime soon or answer your cries for help. You are on your own—and remember: until then, failure remains a punishable offense.

Decades into this digital problem, our citizens still await the simple analog answers to the basic questions of how to "behave" in the face of this national security crisis:

- What must I know?
- What should I do?
- To whom can I turn?
- Where is my 911 for reporting and response?
- Where are my "amber" alerts?
- Why don't I have a neighborhood cyber cop and cyber firefighter?
- Where is my CDC (Center for Disease Control) to control this epidemic?

Posed differently, pretend for the moment you are a criminal, hostile state, terrorist organization, or anarchist. Your escalating goals against our nation and people are relatively straightforward:

- Steal money, business strategies, intellectual property (IP), confidential data, and identities.
- Out-compete our established and start-up companies.
- Leak personal communications to embarrass and impugn the reputations of our leading officials and business executives.
- Waste public and private sector capital and talent on inadequate protections.
- Disrupt corporate and governmental operations.
- Influence elections and public opinion.
- Perpetuate internecine conflict between a government, its citizens, and allies.
- Widely erode trust and confidence in democratic institutions.
- Diminish global competitiveness and influence.

- Compromise military and national security secrets and technologies.
- Destroy vital infrastructure, governmental and business operations.
- Cause death, destruction, widespread economic harm, and panic.
- Ensure, over the longer term, that available talent and resources never come together for mutual protection, mitigation, and recovery.

Could you possibly have found (or hoped for) a richer target with a more divided and fragmented system for defending its people and enterprises?

Here's the cybersecurity message that people are still waiting to hear from their leaders:

"It's the cybercrime and its sponsors (not your cybersecurity), stupid. And we have a plan to address it together for everyone's benefit."

The Digital State of Our Union—What Should Unite Us—

Recognizing the necessity of an informed citizenry to an effective democracy, the late Senator Patrick Moynihan had a simple rule for debating issues of national importance:

> *"You are entitled to your own opinion. You are not entitled to your own set of facts."*

For years, experts have advised that the future of crime, geopolitical conflict, and warfare will be through the portals of cyber. That future is now.

We are at an inflection point where much can be shared—and confessed—about our lack of cybersecurity

and the potential for ongoing, significant, and systemic harm. The risks are global, national, organizational, and very personal. On a bi-partisan basis, officials and industry leaders have forcefully spoken out about our exposures and implored for collective action. Without question, the issue is among the most urgent of threats to national security, the competitiveness of our economy, the safety and confidence of our citizens, and the freedoms that constitute our way of life.

As National Security Director James Clapper explained to our military, "A lot of people find surprising in our post-9/11 world but in 2013 'cyber' bumped 'terrorism' out of the top spot on our list of national threats. And cyber has led our report every year since then."[18]

Although this issue has been with us for almost 20 years, we are no closer to a solution—or even a consensus on how to search for the answers. Across sectors, industries, and allied nations, our efforts have been essentially "stove-piped", ad-hoc, and lacking. Within a political environment where leading issues have their "Czars"—and in a country with no shortage of expertise—the question of responsibility for leading the cyber defense of our nation still has no definitive answer. Inexplicably, even the heat of a presidential contest—fueled by a steady stream of hacks, leaks, "fake" news, and evidence of foreign manipulation of social media—failed to prioritize the issue and the implementation of a national strategy.

No one believes we are prepared. No one believes that we are even heading in the right direction. Our Balkanized approach to cybersecurity extends the definition

---

[18] Aaron Boyd, DNI Clapper: Cyber bigger threat than terrorism, FED. TIMES (Feb. 4, 2016), http://www.federaltimes.com/story/government/cybersecurity/2016/02/04/cyber-bigger-threat-terrorism/79816482/. Homeland Security Secretary Jeh Johnson made a similar point during a keynote speech at CyberCon.

of insanity of doing the same thing repeatedly, and expecting a different result. Leading experts tell us that things are likely to get far worse before they get better.[19] Many continue to fear it will take a "Cyber-9-11" or "Pearl Harbor" event before we wake up to the magnitude of this threat and the need for a consensus approach. (By then, of course, wide-scale irreparable harm will have occurred, and the zero-sum political process of hindsight and blame will have taken center stage.) Even with the benefit of a non-partisan Presidential Commission Report by some of the leading experts in technology and security, we are still no closer to a fix.[20]

As Admiral Michael Rogers, Commander of US CyberCommand testified in a public forum, "It can be difficult to explain the nuance and depth of the threats that we see on a daily basis."[21]

With each passing day, the crisis escalates, with no end in sight. The attacks against us are purposeful. They are growing in volume, speed, efficacy and audacity. The range and goals of the actors are expanding. Their tools are increasingly sophisticated. The personnel and sponsors behind these attacks have demonstrated their capacity to stay a step ahead of even the most sophisticated and hardened defenses. The threat has been compared to that of an iceberg where the majority of the hazard—including those responsible—lurks below the surface of what we can see. Every day provides more lessons that the vectors of attack

---

[19] Michael Hayden, Why Cyber Security Dangers Will Only Get Worse, FIRST REPUBLIC (Sept. 20, 2016), https://www.firstrepublic.com/all-articles/life-and-money-protect-against-fraud/former-cia-director-michael-hayden-why-cyber-security-dangers-will-only-get-worse.

[20] NAT. INST. FOR STAND. & TECH., *supra* note 10.

[21] Statement Of Admiral Michael S. Rogers, S. COMM. ARMED FORCES (Apr. 5, 2016), *available at* http://www.armed-services.senate.gov/imo/media/doc/Rogers_04-05-16.pdf.

are more widespread, smarter, and potentially more damaging than we previously thought. There is no disagreement about our exposures and the worsening storm ahead.

Make no mistake. Our adversaries are agile, highly motivated, and well financed. Global operatives are constantly at work probing our networks, looking for the weakest links in our lines of defense. They possess a growing inter-continental arsenal of software and schemes that can be launched with the single click of a mouse—from anywhere and at any time. FBI Director, James Comey has noted, at the "top of the stack" we see increased efforts at cyber intrusion by nation-states and near-nation-state actors. China, Russia, Iran, and North Korea are the most prominent players. There has been exponential growth in multinational cyber and terrorism syndicates—criminal groups that are increasingly specialized to a role, who are stealing information and offering for sale to the highest bidder the means of destruction, disruption, and embarrassment.[22]

Here is the inconvenient truth about our connected world: the Internet was designed for accessibility and speed—never for security and protection. While it has delivered on its promise of social and economic progress, it has also delivered unparalleled opportunities to those seeking to scale global conflict, terrorism, criminal activity, state and industrial espionage, and vandalism.

Even though the early architects of the Internet came from the Pentagon, they never foresaw the connectivity of devices that one day could be strung together to provide the modern portals for crime, warfare, and geopolitical disruption. Today, it is rare to find a computer or smartphone

---

[22] James Comey, *Humility, Adaptability, and Collaboration: The Way Forward in Cyber Security*, FED. BUREAU OF INVESTIGATION (July 27, 2016), https://www.fbi.gov/news/speeches/humility-adaptability-and-collaboration-the-way-forward-in-cyber-security

that is not linked to another—that has not been probed by a "hackavist", digital criminal, terrorist, or nation looking for weaknesses to exploit for profit, espionage, destruction, or political advantage.

For criminals, rogue states and mischievous actors, the digital world offers low-risk high-reward opportunities for riches and mayhem. It has become the promised land for the perfect storm—with few barriers to entry, a borderless global reach, "virtually" assured anonymity, the unlikelihood of prosecution (even if identified), and, best of all, largely defenseless victims not allowed to fight back.

The tools to wage cyberattacks have become ubiquitous, accessible, and irresistible—from phishing schemes to malware to "botnets" to "chatbots" to global mercenaries for-hire. With cyber warfare now on sale, hacking is both a lucrative business and a geopolitical weapon.[23] The "dark" or "deep" web (where non-indexed information and anonymity thrive) now hosts multiple discount marketplaces for buying and selling stolen data, "off-the-shelf" attack software, and "support" services. Many of these offerings have proven so successful they come with money-back guarantees.

The actors and the methods behind these attacks morph and innovate in mobile and scalable ways that leave our leading enforcement and intelligence officials responding to yesterday's battles. With certainty, tomorrow's channels and attacks will be different and more sophisticated than today's. They will bypass our most informed predictions and exceed our most vivid imaginations. Without collective protections, there is no way for anyone to stay safely ahead.

The finances, trade secrets, communications, and operations of our enterprises, as well as the identities and

[23] Mattathias Schwartz, *Cyberwar for Sale*, N.Y. TIMES (Jan. 4, 2017), http://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html.

privacy of our citizens, remain at constant risk. Digital destruction can come directly or indirectly, through a thousand nicks or a single sucker-punch knockout. The stealth and pervasive nature of these attacks often means that an invasion can take many months to detect, and the damage years to repair, if repairable at all.

With over 100 million Americans' personal data compromised in recent years — including credit-card, tax, and medical records — not surprisingly, the Pew Research Center found that nine out of ten Americans say they feel they have lost control of their personal information and have little confidence in the security of their everyday communications.[24]

Data thefts, distributed denial of service (DDOS) attacks—coupled with extortion schemes—have been successfully launched against governmental agencies, central banks, the media, utilities (including nuclear and water plants), banks, hospitals, manufacturers, law firms, and stock exchanges, just to name a few. Our military and law enforcement agencies have been successfully targeted on a daily basis by state actors and cyber criminals, reflected by the intrusion last year into the Office of Personnel Management (OPM), when the personal information (including fingerprint records) of millions of current and former federal employees was stolen and are now being exploited.

Networks that control critical corporate and governmental infrastructure (power grids, pipelines, manufacturing, communications, health, transportation, refinery, and water) remain under constant probe for vulnerabilities by hackers in Russia, China, Iran, and North Korea, with an eye toward the future and far more damaging

---

[24] Mary Madden, *Privacy and Cybersecurity: Key findings from Pew Research*, PEW (Jan. 16, 2015), http://www.pewresearch.org/key-data-points/privacy/.

intrusions and systemic attacks that can cripple our nation. Our enemies have electronically stolen the plans of advanced defense systems and weaponry—cancelling out years of research and development, and the investment of hundreds of billions of taxpayer dollars. Security specialists recently discovered preinstalled secretive software on Chinese-made phones that can monitor where we go, whom we talk to, and what we write in texts.

Corporate America faces a relentless wave of state-sponsored and criminal hostilities. Whether motivated by financial, ideological, or geopolitical objectives, the cyber targeting of corporations for their proprietary data, communications, and IP is increasingly the modus operandi of hostile state actors. "Ransomware" attacks are spreading like a virus—disabling systems and extorting hundreds of millions of dollars annually from enterprises for restoring access. Leaving corporate targeting unchecked not only poses a significant risk to the sustainability of companies and their labor force trying to compete in a global economy, but also to the inter-connected dependencies of our nation's critical infrastructures and economy.

The Black Hat USA 2016 Conference surveyed its elite network of cyber security experts and revealed that 72% of respondents believed it likely that their organizations must deal with a major data breach in the year ahead. Startlingly, 74% of respondents said that they did not have enough staff to face the threats that they expect to encounter. Even more alarming, 67% of respondents stated that they themselves do not have enough training to do their jobs.[25]

Penetration tests and scans may satisfy regulatory requirements, but they beg the question of how to identify which vulnerabilities actually pose true risks to their

---

[25] *The Rising Tide of Cybersecurity Concern: 2016 Black Hat Attendee Survey*, BLACKHAT (Jul. 2016), https://www.blackhat.com/docs/us-16/2016-Black-Hat-Attendee-Survey.pdf

organizations—and how to stay ahead of the sophisticated means and schemes that indirectly can gain entry though vendors, suppliers, connected devices or even a single employee with access.

For those hoping that at least Uncle Sam (forget his fifty state siblings) can make progress against these threats, here is the reality from the Government Accountability Office (GAO). The number of cyber incidents actually known and then reported by federal agencies has jumped over 1,300 percent (5,503 to 77,183) over the ten years through fiscal 2015—with the situation looming worse for 2017. [26] For sound reasons, companies are increasingly reluctant to entrust their regulators with requested confidential information, out of concern that the government itself maintains insufficient cyber security protocols.[27]

In 2016, prosecutors described the 20 yearlong thefts of 50 terabytes of classified data by NSA contractor, Harold Martin as "breathtaking". Tellingly, Martin's actions followed the lessons learned from the breaches of Edward Snowden and Bradley Manning—notwithstanding the government's expenditure of hundreds of millions of dollars to enhance background checks, detection technology, and the physical inspection of people leaving secure buildings.

Highlighting our worldwide exposures, the Global Commission on Internet Governance explained that in the packet-switched networks and data clouds of the Internet, the communications and data of all parties are mixed

---

[26] Joe Davidson, *Federal cyber incidents jump 1,300% in 10 years*, WASH. POST (Sept. 22, 2016), https://www.washingtonpost.com/news/powerpost/wp/2016/09/22/federal-cyber-incidents-jump-1300-in-10-years/

[27] Andrew Ackerman, *Wall Streeet Frets Over U.S. Cybersecurity*, WALL ST. J. (Nov. 9, 2016), http://www.wsj.com/articles/wall-street-frets-about-cybersecurity-as-u-s-demands-more-data-1478601006.

together.[28] Put in context, we share the same information super-highway for work, school, and play as those seeking to drive home a wide range of threats. Indeed, some have concluded that the entire Internet must be reconstructed if we are ever to contain these actors.

While commerce has always outpaced security protections, now it does so at Internet speed. Our exposures are expanding in lock step with the growing interconnectivity of our networks and devices. We can't yet defend against *yesterday's* means of attacks—nevertheless we continue to innovate and require by regulation tomorrow's greater digital dependencies.

The next phase of the information revolution is the Internet of Things (IOT). It promises to seamlessly weave together all of our technology and data to improve our lives. It will also enlarge our vulnerabilities to attacks by hostile states, criminals, and terrorists. Researchers have shown just how easy it is to take over a car's engine and controls, to secretly turn "smart" phones and devices into machines that spy on our activities, and to convert connected household devices (light bulbs, baby monitors, thermostats, etc.) into a botnet WMD that can disable critical Internet operations.

Anomalously, these policy questions about our nation's cyber security await a fulsome public debate, no less answers:

- *When you already are in a hole, shouldn't you stop digging—or at least pause—and figure a way out?*

[28] Samantha Bradshaw, *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*, CGIC (Dec. 8, 2015), https://www.cigionline.org/publications/combatting-cyber-threats-csirts-and-fostering-international-cooperation-cybersecurity.

- *Where is the analysis that weighs the benefits of our increasing connectivity against the growing costs and risks to national, economic and personal security?*

Experts say this year's massive denial of service attack against Dynamic Network Services, Inc. (DYN)—whose servers manage Internet infrastructure and traffic—offered a glimpse of a new era of warfare and weaponized threats to a super-connected society. The attack relied on malicious software taking control of a network of hundreds of thousands of internet-connected consumer devices (cameras, baby monitors, DVRs and home routers)—to overwhelm Dyn's servers with billions of bytes of unwanted data and disable over 1,200 websites. An expanded use of this same malware was apparently used to target routers made in Taiwan and disable a million Deutsche Telecom customers.

While the government has yet to determine responsibility, this much is known:

- The exploitation of IOT will continue. Similar or more damaging attacks could occur tomorrow and we are powerless to stop it.[29]
- Anyone can buy the capabilities used in this attack for less than $1,000
- Hostile nations and sophisticated hackers are capable of far worse—and there are tens of millions of insecure devices that, if harnessed, could cause incredible disruption.
- Any threat of a counter-hack or physical attack seems to be an ineffective deterrent.

[29] FBI Private Sector Bulletin (October 26, 2016)

In 1710, the satirist Jonathan Swift observed how "falsehood flies and the truth comes limping after it." Now it digitally circles the globe before truth even finds its keyboard.

In early October 2016, cyber warfare claimed public trust in our electoral process and free press as a geopolitical casualty. The nature of these hacks and leaks reflected a clear escalation in geopolitical digital warfare—an organized cyber effort to divide our citizens, break our democratic bedrock, impede our ability to govern, and diminish our reputation abroad. Regimes that have little to offer the world can now create the digital havoc and falsehoods to diminish democracy in the eyes of a global public and challenge Churchill's truism that "democracy is the worst form of government, except for all the others." As the New York Times reported shortly before our presidential elections, regardless of who wins, "America's image stands tarnished in the eyes of its own people and the world."[30]

Experts already have pointed out that it would take little for hackers to reach our online voting machines and affect election returns. Incongruously, even after another close national election in which the popular and electoral votes were split and local outcomes mattered greatly (and 16 years after under 600 recounted votes and a divided Supreme Court decided a Presidential election), our nation still "ensures" the peaceful transition of power through repair-prone machines with obsolete software and known security holes. As the recounts reminded us, pretending the problem doesn't exist only feeds the growing concerns of many Americans that the system is rigged and that their votes don't count.

---

[30] Farah Stockman and Nick Corasaniti, *Forget the Cost to the Candidates. This Campaign's Cost America More*, N.Y. TIMES (Nov. 5, 2016), https://www.nytimes.com/2016/11/06/us/politics/world-reaction-campaign.html.

Authorities are now bracing for a future filled with state-sponsored "surprises" that will seek to foment civil and social unrest. As more individuals rely on online sources to stay informed—and because the Internet and its social platforms do not discriminate between credible and unreliable sources—artfully propagandized information can quickly scale to yield long-lasting political advantage. Increasingly, when it comes to hacked information and our social media platforms: *If it bleeds, it leads, reads and gets believed*.

Simply summarized, governments, businesses, and individuals are now grounded in a new reality of inevitability and resignation about their interconnected vulnerabilities. In sobering public statements, senior national security and law enforcement officials have now conceded that that it is simply unrealistic to expect the prevention of breaches at their agencies. Regardless of sector or enterprise, even the most expensive and expansive efforts at prevention and detection will prove only partially effective— more useful in temporarily delaying the inevitable or deflecting the risk to another enterprise that offers less resistance.

Throughout our public and private sectors, people are rightfully asking themselves, "How fast do I have to be to outrun this bear?". In the short term, the answer might be just slightly faster than the other guys. In the longer term, this bear continues to hunt and won't hibernate. It is looking for everyone.

Collectively and collaboratively—for the safety of all—this growing risk must be contained, scared away, and hunted down.

A Declaration of Interdependence

Our Founding Fathers knew that the decision to issue the Declaration of Independence could not stand on its own. To ensure public support, they carefully explained the

necessity and rationale for this call to action. They also included a list of specific "grievances" that outlined why separate colonies and diverse interests had to unite to change their governance—and free them from the tyranny that threatened their security and freedoms.

While we have yet to convene a *Continental Cyber Congress*, experts across our country have, in various forums, enumerated what amounts to a list of grievances about the online threats to our nation's security, economic competitiveness, and the protected rights of our democracy. These increasing threats and burdens now necessitate a change in our digital governance.

For too long, the costs of defending ourselves have constituted *taxation without the representation* that we will be safe or even more secure.

If reduced to a formal document, this *Declaration of Interdependence* would, in part, *hold these (digital) truths to be self-evident*:

- Cybersecurity is our nation's *black elephant* threat — a dangerous crossbreed between the "black swan" risk (capable of producing unexpected outcomes with enormous consequences) and the "elephant in the room" (a large problem that hides in plain sight from solutions). Every day brings new reminders about how it moves, morphs and metastasizes—and cannot be managed alone.
- All of us are at risk, all of the time. As acknowledged by our law enforcement and national security leaders, there are now only three types of enterprises left in this nation: Those that have been hacked, those that will be hacked, and those that already have been hacked but don't yet know it. No longer is it a matter of "if". The only open questions are when, where,

how, how bad—and whether recovery is even possible, despite time and expense.

- Long ago, cybersecurity transcended the risk management and response capabilities of any single community — technology, military, intelligence, law enforcement, academic, or business. No group or entity can have all the answers or even a claim to superiority. Global actors are starting to use artificial intelligence to test the vulnerabilities in our systems and innovate the next means of attack. Only a broad collective effort can hope to stay ahead of this organized and ongoing threat. Together, our expertise and resources can be formidable. Apart, we remain highly vulnerable.
- "If you can imagine it, they can do it. And even if you can't imagine it, they have — and already are working on it." There now exists a seemingly limitless supply of sophisticated global talent, state-sponsorship, and innovation waiting to be deployed to support intrusion, theft and destruction. The United Nations estimates that 80 percent of it is from highly organized and ultra-sophisticated criminal gangs. [31] This skilled pool is growing deeper every day and there are few barriers to entry. No different than when new deposits of energy and precious metals are discovered, the success and growth of the cybercrime "mining" industry will continue to attract people and resources worldwide. Trying to manage these emerging risks without

[31] *Caleb Barlow: Where is cybercrime really coming from?*, TED TALK, http://www.ted.com/talks/caleb_barlow_where_is_cybercrime_really_coming_from/transcript?language=en#t-104997.

an organized national effort is like the comedienne Lucille Ball trying to box the chocolates speeding off the factory's conveyer belt.[32]

- A large catastrophic and systemic attack is no longer hypothetical. There is no shortage of actors, ways, or means capable of launching systemic strikes against critical infrastructures—defense, power, transportation, telecom, water, medical, and financial. The direct and collateral consequences of such attacks, renders irrelevant any prospect of individualized security protection. We all share in the exposure. We all must share in the solutions.
- In reality, we are witnessing the early stages of a highly asymmetrical and multi-front war—in which ground troops, tanks, aircraft, and ships will be of little defense. These coming waves promise to be far more than any one enterprise, sector, or even country can handle. Do we have a national plan to address this crisis and respond if a major event occurs? As Eric Schmidt and Jared Cohen of Google recently warned: "We must prepare ourselves for the wars of the future…cyberattacks and online disinformation campaigns will define the next generation of conflict, and they will unfold silently, invisibly and relatively inexpensively. It's now incumbent upon policymakers and tech

[32] History104WWU, Lucy's Famous Chocolate Scene, YOUTUBE (May 19. 2010), https://www.youtube.com/watch?v=8NPzLBSBzPI

companies to help keep our information secure and infrastructure safe."[33]

- We are now locked into a defensive and offensive arms race. Hackers have always seen the benefit of sharing information and partnering. They have embraced open-source collaboration and the free-flow exchange of malware, phishing schemes, bots, and talent. It is how they have stayed a step ahead of law enforcement efforts. We also must share and collaborate if we are to contain our threats and prepare for tomorrow. As experts have noted, many effective security tools and resources already exist. "Where we need to make progress is in applying these tools and defenses at scale."[34]
- Today, for fear of being exposed, many financial services firms are reluctant to share information about cyber-attacks. However, with blockchain and other technologies, they could confidentially share threat data in real time that could be used to spot patterns and quickly develop countermeasures.[35]
- In our interconnected world, even a single intrusion can carry systemic consequences. Think of this digital issue as like the physical risk of fire—where a small flame not quickly detected and extinguished can quickly grow into

---

[33] Eric Schmidt & Jared Cohen, *We Must Prepare Ourselves for the Cyberwars of the Future*, TIME (DEC. 19, 2016), http://time.com/4606057/cyberwars-of-the-future/.

[34] *Id.*

[35] Steve Hamm, *Blockchain: Securing the Financial Systems of the Future*, IBM: THINK BLOG (May 16, 2016), https://www.ibm.com/blogs/think/2016/05/blockchain-securing-the-financial-systems-of-the-future/

an inferno that engulfs an entire community. In epidemiological terms, attack “viruses” carry infectious contagions that can quickly and silently spread from user to user, network to network, sector to sector. Unfortunately, we have yet to address our exposures to cyber threats, as we have to fire and disease.

- We are only as strong as our weakest links and points of “infectious” contact. These points of contact include our global chains of suppliers, customers and partners—and the single employee or family member who may unwittingly click-open a phishing scheme. We have found the ways to ensure the safety of our supply chains of food, drugs, and consumer products. We still await similar governmental protections to address our chains of cyber connectivity.
- Our passwords are the keys to our digital castles. They are also among the weakest links in our security chain. As Michael Chertoff, former Secretary of Homeland Security, has noted: in every "major headline" breach, the attack vector has been the common password. Indeed, passwords themselves are often the most valuable treasure for attackers and easily obtainable, given how many people reuse passwords between accounts. We need to acknowledge the failure of passwords and make it a national priority to come up with something better – leveraging the next generation of authentication technologies to authenticate identities in a way that is both

stronger than passwords and also easier for people to use.[36]

- Expertise must be available to all—not just to the well-resourced. We must end the game of "robbing Peter to pay Paul". Cybersecurity cannot continue as a zero-sum competitive sport, involving talent and resource recruitment wars that make some stronger but still leave all of us vulnerable.
- The integrity of our democracy and the unity of our nation are now at stake. Make no mistake about the disruptive capacity of this threat. Highly sophisticated forces have shown themselves to be adept at deploying digital jiu-jitsu to exploit our rights of privacy, press, speech, travel, and commerce. They have directed the theft of sensitive records and communications, disrupted the operations of leading media outlets and compromised their confidential sources, hired armies of trolls to plant self-serving messages in the comment sections of our press,[37] taken control of their own television stations, deployed "chatbots" to influence social media with fake news and propaganda, and leaked stolen emails through various organizations such as WikiLeaks. Their

[36] Michael Chertoff, *Passwords are the weakest link in cybersecurity today*, CNBC Oct. 6, 2016), http://www.cnbc.com/2016/10/06/passwords-are-the-weakest-link-in-cybersecurity-today-michael-chertoff-commentary.html

[37] Caitlin Dewey, *Hunting For Paid Russian Trolls In The Washington Post Comments Section*, WASH. POST (Jun. 4, 2014), https://www.washingtonpost.com/news/the-intersect/wp/2014/06/04/hunting-for-paid-russian-trolls-in-the-washington-post-comments-section/?utm_term=.bd5b9cfb8daf.

goals could not be clearer—discredit, divide and diminish our nation.

- Cybercrime remains a "virtually" perfect crime and act of war. Low risk and high reward—it is mobile, cheap, anonymous, and remotely scalable. Easily cloaked and launched from safe havens, the attacks carry little risk of detection, prevention, apprehension, or punishment. Unlike conventional warfare and crime—which are waged on land, sea, and in the air—finding and fighting a digital enemy that reveals neither a face nor wears a uniform is far more difficult.
- Trying to fight off these foes without a common defense is akin to the punishment imposed upon *Sisyphus*—condemned by the gods to repeat forever the task of pushing a boulder up a mountain, only to see it roll down again and again. As Albert Camus might have observed, our absurd paths around cyber no less reflect a futile search for meaning, unity, and clarity in the face of an unintelligible world.[38]
- Unfortunately, the fog of cyberwarfare means there are no satellite images to bring to the UN to rebut denials of missile deployment in Cuba. Attributing digital responsibility and motive involves part science, part forensic art, and part intuition. It can also require withholding proof from the public, lest we jeopardize the very sources and methods (humans and technology) that maintain ongoing national security capabilities. With criminals not being physically present at the scene of the crime, there is no dusting for fingerprints, scraping for DNA, or

[38] ALBERT CAMUS, THE MYTH OF SISYPHUS, *available at* http://dbanach.com/sisyphus.htm.

security videos to review. At best, we strive for "highly confident" conclusions based on such circumstantial evidence as data logs, motive, type of scheme, malware used, device and data locations, language, online chatter, and even the hours when the crimes are committed. Unfortunately, post-Iraq, the general public (and many officials worldwide) view US intelligence conclusions with skepticism, even in the face of otherwise overwhelming proof.

- We still lack overall visibility into the true cyber threat environment and what we should be defending against. In an era of limited resources, many practitioners are understandably frustrated with the lack of guidance about how to "know" and prioritize (triage) the actual threats to their organizations. They are in the dark about the actors that may wish them harm and how to best defend against them. Too often we have enlisted our people and resources to focus on regulatory compliance and yesterday's battles—in the misplaced hope it would equate to security. More often than not, this has done far more to foster adversarial relations between the government and the private sector than diminish the recurring nature of this threat.
- In reality many of our most consequential threats emanate from a relatively discrete group of states, state-sponsored actors, and state-protected groups. Attacks are often backed or protected by state sponsors and highly organized groups (criminal and terrorist), with local power and influence. Solutions must reflect these geographic and geopolitical realities.
- Those behind cyber-attacks may be criminals, spies, terrorists, "hacktavists", and "rogue"

states, but they are rational actors and they remain incentivized. The infamous 1930s bank robber, Willie Sutton, reportedly offered a simple explanation to why he robbed banks: It's where the money is. Whether as an outsider breaking in or as an insider attacking from within, our connected networks will continue to offer the digital keys to the castles containing, among other assets, money, state and military secrets, IP, political propaganda, business strategies, market-sensitive information, private communications, personal identities, legal advice, and reputational issues. With so much to gain and so little to lose, why should they stop?

- Contrary to our other law enforcement models, we have not accepted cybercrime into our successful paradigms for community safety. Victims have unfairly shouldered the burden, blame, and liabilities for being attacked—yet are faulted for not coming forward to report and cooperate. There have been no police or fire departments for protection and response, no clear compliance codes for safety and security, no training for prevention and resiliency, no "safe harbor" protections for the compliant and law abiding, and no means of recourse to pursue justice and recover damages. Online and offline, we still await a "cracked" *Windows* approach to policing the Internet and containing the actors intent on causing us widespread harm.
- To date, our international laws and treaties have not kept up with our digital exposures. We lack the legal framework to reach, punish, and deter the global perpetrators—no less the "Geneva Convention" ground-rules to control digital warfare and geopolitical conflict. Significantly,

diplomacy has so far yielded few protections, if any. Without formal treaties, laws, and the effective means for enforcement and international cooperation, responding to this risk will remain like trying to defeat the game of *whack-a-mole*.

- We still need a legal and policy framework to "offensively" respond to this risk. To date, we have essentially played only defense. This approach requires being perfect 100% of the time—while the "bad guys" need succeed once and enjoy the "free option" of continuing to try. Going on offense requires rules and lines of responsibility for carefully balancing the common (and often competing) interests of the public, private, and civilian sectors. This process must closely weigh such factors as certainty about the target, likelihood of success, collateral harm, potential for escalating conflict, the exposure of our own capabilities, and unintended consequences. Admittedly, the playbook for offense may be complex, but defense-only play calling has been *simply* ineffective and unsustainable.
- We have yet to unpack (no less debate) a number of difficult national security questions at the heart of this risk, including:
    - Are government officials purposely not disclosing known security gaps in software and systems, lest they compromise their own (offensive and defensive) cyber activities and capabilities?
    - Are government officials aware of the means and timing of some attacks and the actors, but, under the rubric of national

security, withholding information that could prevent or mitigate the damage?
    - Don't we need to distinguish between "traditional" criminal activity that may be susceptible to more "traditional" law enforcement solutions and the attacks that are geopolitically inspired acts (e.g., espionage and sabotage) that require diplomacy and military responses?
    - Can we separately address the attacks (and attackers) that are part and parcel of a *quid pro quo* game between competing nations?
    - What criteria should be used to answer these questions, and who is making these decisions?
    - How should the costs of these decisions be borne?
    - If the big guys are bowling, does this make us the unwitting pins? If so, shouldn't someone be setting us back up when we get knocked down?
- At the very least, we must address the "detection gap". Speed matters. Lack of speed kills. On average, it takes 150+ days before enterprises even realize that they have been breached—and another 50-100 days to mitigate the breach. It is the functional equivalent of thieves being able to secretly live in your home or office and having half a year to sort through and take your most precious belongings——leaving you needing several more months to even know what is missing and which locks must be changed. Worse still, institutions often now only learn of a hack by chance—*e.g.,* through outside parties working on separate matters (law

enforcement, security consultants, the media, or compromised customers). It need not be this way. Collaborative solutions can help contain the damage by narrowing the time between an attack and detection.

- Globally, we are losing unprecedented amounts of money, information, intellectual property, and state secrets — much of it to support hostile regimes and criminal organizations. Hacking, leaking, denial-of-service attacks (DDOS), and ransom-ware have become big business for cybercriminals and their state sponsors. Criminals have stolen billions of records and caused hundreds of billions of dollars in damages—and those are just the breaches we know about. Whether the attacks come from outside an organization, or from an "insider threat", an overview of some of the *disclosed* breaches proves sobering about the nature and extent of our shared exposures.[39]

[39] Introduction of attack malware into NASDAQ's systems (2010); Theft of Wyndham Hotels' customer data (2012); Massive destruction of Saudi Aramco data (2012); Edward Snowden's national security disclosures (2013); Theft of high-'s customer data (2013); Attacks on networks—the New York Times, Bloomberg, French national television (2013); North Korea's cyberattack on Sony Pictures (2014); Chinese ("Ugly Gorilla") theft of security data of US utilities (2014); Theft of Home Depot's consumer data (2014); The hack of the White House's systems (2014); Hackers Steal Data on 500 Million Yahoo Users in 2014 (disclosed: 2016); Penetrations of Nuclear Regulatory Commission (2014-present); Breach of credit card terminals at 33 PF Chang's restaurants; Theft of U.S. government personnel data (2015); Anthem's and Ashley Madison's loss of confidential client information (2015); Penetrations of Breach of NASA's data (2015); Theft of billions of dollars from banks—U.S., China, Russia, Greece, etc. (2015); Damage to French Utility(2015); Exploitations of the SWIFT system, various banks and the Federal Reserve (2016);Theft of nearly $100 million from the Bank of Bangaladesh (2016); Disabling of the

- The losses are growing. The consensus annual *hard-dollar cost* of cyber-attacks to the global economy now exceeds $445 billion— more than the GDP of 160 nations and more than the market cap of Amazon, Facebook, or ExxonMobil.[40] Yet, the "whisper" number of true damages dwarfs this estimate. Many successful intrusions are never detected. Other attacks go unreported, and the lessons are not shared due to national security considerations and business concerns over client relationships, litigation, and reputational harm. Often the reported losses fail to reflect the "soft-dollar" expenses of internal resources, business interruption, and lost corporate opportunities.
- The costs of cyber security effectively represent the extortion of a national "protection tax". Throughout our public and private sectors, we have paid billions of dollars in recurring and spiraling security and compliance costs simply to stay in business—with no guarantee of safety or even a return on the investment. The need for protection has also "taxed" the streams of global

---

Ukrainian power grid (2016); Iran's hack of a New York's water system (2016); Attack on German Nuclear Facility to gain remote access (2016); Thefts from cryptocurrency (bitcoin) exchanges (2016); Ransomware attack on Hollywood Presbyterian Medical Center (2016); Leaks of Mossack Fonseca's client communications ("Panama Papers") (2016); Data breaches of the National Security Agency (NSA) and NATO (2016); Hack of White House Personnel (2016); Theft of World Anti Doping Agency data on 25 more athletes (2016); Hack of the communications of the Democratic National Party and various political officials (2016); denial of service attack on Internet infrastructure company Dyn (2016).

[40] Net Losses: Estimating the Global Cost of Cybercrime, MCAFEE (Jun. 2014), https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2-summary.pdf.

commerce and innovation—disrupting trade relationships, investments, acquisitions, partnerships, and job creation.

- Insurance is only providing a partial answer. The insurance market is still in its relative infancy. Policies generally have low limits and numerous exclusions. To increase the amount and scope of coverage, carriers still need better actuarial data and intelligence regarding the cyber risk profiles of the companies they insure and the steps that can be taken to mitigate those risks. Government backstops for a systemic attack may also be needed.
- Our past mistakes need not be repeated. Over ten years ago, the 9-11 Commission shared two principal findings about a previously new threat and means of attack that "changed everything"[41]: 1) Just because events come as a shock, doesn't mean they arrive as a surprise and 2) Even our most consequential threats can be prevented or mitigated with the benefit of shared recognition, shared intelligence, and shared action. It is time to apply these lessons to the management of our digital threats. No "big bang" event required.

For these reasons, and many more, we have reached our "breaching" point. Approaches and incentives must align for protecting the broad public interest.

Back to the Future—An Analog Approach To Our Digital Security

[41] THE 9/11 COMMISSION REPORT, *available at* http://avalon.law.yale.edu/sept11/911Report.pdf.

Within non-stop news cycles and the hair-on-fire moments of breaches and leaks, it has been far too easy to lose our "true north" positioning of this threat and its sources—and thus overlook our opportunities for immediate and long-term protections.

Almost 250 years ago, scattered colonies came together because of words and ideas that answered our shared exposures with empathy, utility, simplicity, and the recognition of common interest in the public good. The authors understood the need to clearly convey the state of our affairs, the conditions that required unity of action, and the ideas and values that could sustain and protect us over the long-term. Their goal: a nation indivisible.

Our founders began an experimental nation with less-than-perfect but resilient models that could be improved upon over time to provide even greater protections. Remarkably, they did so without the need for complex regulations, large fines, investigative hearings, press conferences, or class-action litigations —no less a national disaster.

No single individual did more to advance these principles of problem solving and mutual aid than Benjamin Franklin. He did so through the institutions he innovated and the ideas he openly shared. While addressing a wide spectrum of issues, Franklin's ideas were governed by a consistent approach to problem-solving and the public good:

- Shared problems deserve shareable and scalable solutions
- To be effective and accepted, solutions must be based on empathy, utility, and simplicity for the users
- Solutions must be resilient. They must remain "open source" and transparent—to encourage mutual "ownership" and improvements by others

Franklin's overarching message was simple and straightforward: "The good we can do together exceeds what we can do individually." He refused to patent his works, believing "as we benefit from the inventions of others, we should be glad to share our own…freely."

Franklin's "open-source" ideas merit a timely summation:

- The public library: to provide access to the information that could educate citizens and resolve the pressing issues of the day. Books were scarce and too expensive for the average person to own individually. Led by expert book curators and underwritten by its members (and then taxpayers), the library offered shared access to trusted references and authorities. Reading became "fashionable" and discussion groups popped up throughout the colonies. Americans became known as among the most informed people in the world.
- The local fire department: to respond to the known but unpredictable risks of fire. Franklin recognized the shared nature of this risk and the capacity of even small fires to grow and engulf entire communities. He advocated a common voluntary resource for equipment, training, and personnel that would quickly come to the aid of all. Fire departments soon became a mainstay community institution everywhere.
- A national postal service: to ensure the secure and cost-effective delivery of ideas between disparate people and places. Franklin studied every mail route to re-engineer the Crown's inefficient and insecure system, that was also too expensive for the majority of colonists. Franklin's re-invented postal network quickly

proved reliable, secure, and affordable, becoming popular and profitable. Failure to stay current in picking up your mail was even seen as a breach of a citizen's duty. Those who were derelict were named and shamed in local newspapers. If still unresponsive, they were subject to a penny fine. (Hence: "A penny saved is a penny earned".)

- The public hospital: to ensure that the indigent sick would still have care. Franklin knew those who could not afford medical treatment (or did not know better) posed a risk not only to themselves, but to the broader community. (Analogously, a single cyberattack or the negligence of one person can spread significant harm to us all.)
- A mutual insurance company: to offer policies to help businesses and households manage the ever-present risk of a fire. The company also underwrote mortgages to promote building and recovery efforts, and advanced safer building codes to mitigate the risks. (Insurance was predicated on compliance with these codes.)
- The "Franklin" stove: to offer families and businesses the means for safer and more efficient heating and cooking. Launched as a "minimally viable product" (MVP), the stove was improved upon by others and marketed under Franklin's name.
- Bi-focal glasses: to make it easier for people to simultaneously see from afar and up close. By combining near and far-sighted magnifications into a single split lens, people no longer had to carry two pairs of glasses.
- The lightning rod: to protect buildings against the known, devastating, and unpredictable risks of

> lightning strikes. This inexpensive, utilitarian device safely attracted and deflected lightning's powerful electrical currents away from a structure and into the ground. (On July 4, 2016, Franklin's lightning rod saved Philadelphia's landmarked City Hall from the damage of a direct lightning strike.)

Franklin also offered this advice that feels prescient to the digital age: "*By failing to prepare, you are preparing to fail . . . You may delay, but time will not."*

We submit that Franklin's ideas and institutions help provide the missing blueprint to confront our shared and evolving cyber risks.[42] The criminal and geopolitical nature of cyber-attacks demands sharing information and resources across all sectors—without shame, stigma, or liabilities. Through words and actions, we can message and build what has been missing to date—empathy, trust, utility, and simplicity—and, in turn, the partnerships and collaborative institutions to scale the effective management of this risk. As FBI Director Comey has acknowledged, we need humility, deference and mutual respect in the face of this risk. No one can afford to go it alone.[43]

Reflecting Franklin's philosophy of problem-solving in the public interest, here are some of the shared "*utility centers*" for information, expertise, and resources we can build together with brick and mortar and online:

- Franklin Cyber Libraries: to respond to the need for shared access to the best information and

[42] Peter Beshar, *Benjamin Franklin's cyber solution*, THE HILL (SEPT. 8, 2016), http://thehill.com/blogs/congress-blog/technology/216410-benjamin-franklins-cyber-solution

[43] Comey, *supra* note 20.

resources. These centers would also host training, continuing education, bench-marking, thought-leadership, and industry events. They would further serve as a repository for the contribution of content, data, products, research, and for ideation and collaboration.

- Franklin Cyber Fire Departments: to provide a shared resource to respond to attacks and their contagion risks. The departments would assist in establishing specific safety codes, training protocols, best practices, inspections, table-top attack drills, and help design and test new products for detection, prevention, and mitigation. Similar to our fire code and inspection protocols, safe harbor protections would be established for the compliant. These departments would further serve as repositories of data (identified and anonymized) on attacks and responses. To foster reporting and situational awareness, people would have a simple system for reporting "cyber fires" that could include anonymity protections—no different than how we now deploy "911".[44]
- Franklin Cyber-Postal Services: to ensure the secure and timely delivery of risk-relevant information. It would be a networked service to

[44] Peter Beshar, executive vice president and general counsel of the Marsh & McLennan insurance companies, has specifically highlighted Franklin's approaches to the risk of fire as offering a framework for the management of our cyber risks, *supra* note 37. *See also Internet Needs 'Cyber Fire Department' to Protect Web Users, Claims Vint Cerf*, COMM. ACM (Sept. 6, 2013), http://cacm.acm.org/news/167516-internet-needs-cyber-fire-department-to-protect-web-users-claims-vint-cerf/fulltext ("The Internet needs a cyber fire department to keep risks found on websites and services from spreading, says Google chief Internet evangelist and ACM president Vint Cerf.").

ensure that people and enterprises are informed about the risks and what can be done. In the spirit of Franklin's "penny saved is a penny earned", people who joined this network and acted on the information could be *rewarded* with "safe harbor" liability protections and insurance and product discounts.

- Franklin Cyber Hospitals: to offer trusted centers for diagnosis and treatment of cyber-related attacks and potential viruses, and to treat victims and limit contagion risk. The centers would also focus on preventive medicine and cyber surgery innovation. The hospitals would further serve as repositories for training, data, and innovation. Patient confidentiality rules would be implemented to encourage self-reporting and facilitate treatment. Expenses could be reimbursed privately or through insurance.
- Franklin Cyber-Insurance Centers: to ensure that necessary protections exist to cover the full range of episodic and systemic risks to people, property, and enterprises. The Center would also help compile the actuarial data and risk models for policies and pricing. Similar to existing insurance industry platforms, the center would also offer resources and guidelines for best practices covering prevention, risk mitigation, disaster and continuity planning, industry codes, and sponsor product innovation.
- Franklin Cyber Laboratories: to independently test and certify the cyber safety and security of products—similar to the successful model of Underwriters Laboratories in certifying the safety of our electrical devices since 1894. The "Cyber Lab" would also help incubate products and ideas to respond to the evolving nature of our

> risks—the lightning rods to safely diffuse and ground the attacks, the "stoves" to offer greater safety and efficiency in our connected lives, and the bifocal glasses to help view the near and far away risks.

Details of this initiative must be worked out—but here are some starting points for a framework:

- The utility centers would be organized horizontally, by industry, to best leverage expertise, relationships, facilitate trust, and respond to special needs. Acknowledged experts (curators) with deep domain and industry experience and proven records for collaboration and problem solving-would lead. Analog models include our specialty schools, hospitals, libraries and research centers, and Wall Street's model for specialized banking and research coverage by industry.
- The government would incubate this effort to give it a jump-start. Ownership and operation would be shared, however, between the government, private, and academic sectors on a mutual basis. The centers would operate on a wholly non-political basis. Oversight would come from a duly elected board of directors. Ongoing financial support would come through government funding, member and industry support, and strategic sponsorships (e.g., corporate and insurance).
- Curated products would be made widely available—preferably on an "open-source" basis, to allow for broad input on improvements. Research and distribution would be subsidized where necessary.

- Evidence-based data would be collected to understand the cost-benefits of our efforts—where we were succeeding and where we were failing. The effort would utilize social media to communicate ideas and gain feedback in real time.
- Safe harbors would be an important objective. These industry centers would provide codes of best practices, inter-industry benchmarking, and standards for ongoing care and review. No different from the analog world of fire and disease prevention, there would be liability protections and favorable insurance rates for the compliant, and fines reserved for those who are not.
- To encourage information sharing, mutual confidentiality protections would be established within particular forums similar to the Chatham House Rule, attorney-client, and doctor-patient privileges. Security clearances would be available to provide special access to particularly sensitive information and resources.
- If a national crisis occurred, these centers could be quickly mobilized to respond.
- Opportunities for collaboration and scalability would build upon (learn from) existing non-profit, public-private sector information sharing models such as:
    - National Institute of Standards and Technology (NIST) (formerly, the National Bureau of Standards)[45]

[45] Cybersecurity Framework, NAT. INST. OF STAND. & TECH., https://www.nist.gov/cyberframework.

- Infraguard (FBI's private sector information-sharing partnership)[46]
- The District Attorney for New York County and the City of London's Police Global Cyber Alliance (GCA)[47]
- Financial Services Information Sharing and Analysis Center (FS-ISAC)[48] e
- Legal Services Information Sharing & Analysis Organization | F[49]
- E-ISAC | Electricity Information Sharing & Analysis Center[50]
- Underwriters Laboratories[51]

Conclusion

True security will never be found by signaling through either words or actions that *this* national crisis is different from the past. You are essentially on your own. It is every person for themselves, and you are at fault if victimized by well-armed, well-financed, and well-protected global actors.

By drawing upon our nation's foundational thinking—and some of the ideas that followed—we can "go back to the future" and recast our approaches to cybersecurity with empathy, utility, and simplicity to offer greater protections for the common good.

---

[46] *Infragard*, https://www.infragard.org/
[47] *Global Cyber Alliance*, www.globalcyberalliance.org/.
[48] *Financial Services Information Sharing and Analysis Center*, https://www.fsisac.com/
[49] *Legal Services Information Sharing & Analysis Organization*, https://www.fsisac.com/ls-isao
[50] *Electricity Information Sharing and Analysis Center*, https://www.esisac.com/
[51] *UL*, http://www.ul.com/

While many efforts are already underway within both the private and public sectors, it is now time to accelerate and scale the shared understanding of this threat and the platforms for shareable solutions. Near and long-term solutions will require mutual trust and collaboration by all sides—not stigma, shame, and regulatory schemes focused primarily on punishment.

History rightfully delivers a harsh judgment for when we fail to protect the public against known and consequential harm—when the complexity of our risks is not reconciled with the simplicity of shareable solutions. It is a single word verdict that "mashes-up" the words "complexity" and "simplicity".

The word is *complicity*.

As in the past, we are all in this one together. Our nation and democracy are under attack. None of us is truly safe, unless all of us are. In reality, it's the cybercrime and its global sponsors—not our individual security failures—that is our problem, "stupid".

We must solve this one together.