PewResearchCenter

NUMBERS, FACTS AND TRENDS SHAPING THE WORLD

FOR RELEASE OCTOBER 29, 2014

Digital Life in 2025

Cyber Attacks Likely to Increase

Experts believe nations, rogue groups, and malicious individuals will step up their assaults on communications networks, targeting institutions, financial services agencies, utilities, and consumers over the next decade. Although most expect there will be more attacks, many predict effective counter moves will generally contain the damage. Some say there is now and will continue to be a 'Cold War' dynamic that limits severe harm due to the threat of mutually assured disruption. Some say the threat is 'exaggerated.'

FOR FURTHER INFORMATION ON THIS REPORT:
Lee Rainie, Director, Internet Project
Janna Anderson, Director, Elon University's Imagining the Internet Center
Jennifer Connolly, Research Consultant
202.419.4500
www.pewresearch.org

RECOMMENDED CITATION: Pew Research Center, October 2014, "Cyber Attacks Likely to Increase"
Available at: http://www.pewInternet.org/2014/10/29/cyber-attacks-likely-to-increase/

About This Report

This report is the latest in a sustained effort throughout 2014 by the Pew Research Center's Internet Project to mark the 25th anniversary of the creation of the World Wide Web by Sir Tim Berners-Lee (The Web at 25). It includes the responses of hundreds of experts to a question about the likelihood of major cyber attacks in the coming decade. It is part of a series of reports tied to the Web's birthday; some of the studies look at how far Internet use has penetrated American life and some examine experts' assessments of the technology environment by 2025. The findings we describe in this report emerge in the context of these earlier reports:

- A February 2014 report from the Pew Research Center's Internet Project tied to the Web's anniversary looking at the strikingly fast adoption of the Internet and the generally positive attitudes users have about its role in their social environment.

- A March 2014 *Digital Life in 2025* report issued by the Internet Project in association with Elon University's Imagining the Internet Center focusing on the Internet's future more broadly. Some 1,867 experts and stakeholders responded to an open-ended question about the future of the Internet by 2025.

- A May 2014 *Digital Life in 2025* report on the Internet of Things from Pew Research and Elon University examining the likely impacts of the Internet of Things and wearable and embedded networked devices. A majority of the more than 1,600 respondents said they expect significant expansion of the Internet of Things, including connected devices, appliances, vehicles, wearables, and sensor-laden aspects of the environment.

- A July 2014 *Digital Life* report on "Net Threats" (challenges to the open Internet) from Pew Research and Elon University canvassing a number of experts and other stakeholders on what they see as the major threats to the free flow of information online. A majority of these experts expect the Internet to remain quite open to sharing but they see many potential threats to this freedom.

- An August 2014 *Digital Life* report on "AI, Robotics, and the Future of Jobs" from Pew Research and Elon University about the degree to which technology advances might destroy more jobs than they created. The expert respondents were split on the verdict.

- An October 2014 *Digital Life* report on "Killer Apps in the Gigabit Age" from Pew Research and Elon University about the potential new digital activities and services that will arise as gigabit connectivity—50 to 100 times faster than most Americans now enjoy—comes into communities.

This report is a collaborative effort based on the input and analysis of the following individuals.

Lee Rainie, Director, Internet Project
Prof. Janna Anderson, Director, Elon University's Imagining the Internet Center
Jennifer Connolly, Research Consultant

Find related reports about the future of the Internet at
http://www.pewInternet.org/topics/future-of-the-Internet/

About Pew Research Center

Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping America and the world. It does not take policy positions. It conducts public opinion polling, demographic research, media content analysis and other empirical social science research. The center studies US politics and policy views; media and journalism; Internet and technology; religion and public life; Hispanic trends; global attitudes; and US social and demographic trends. All of the center's reports are available at www.pewresearch.org. Pew Research Center is a subsidiary of The Pew Charitable Trusts.

About the Imagining the Internet Center at Elon University

The Imagining the Internet Center's mission is to explore and provide insights into emerging network innovations, global development, dynamics, diffusion and governance. Its research holds a mirror to humanity's use of communications technologies, informs policy development, exposes potential futures, and provides a historic record. It works to illuminate issues in order to serve the greater good, making its work public, free and open. The center is a network of Elon University faculty, students, staff, alumni, advisers, and friends working to identify, explore, and engage with the challenges and opportunities of evolving communications forms and issues. They investigate the tangible and potential pros and cons of new-media channels through active research. The Imagining the Internet Center sponsors work that brings people together to share their visions for the future of communications and the future of the world.

Table of Contents

Summary

The Internet has become so integral to economic and national life that government, business, and individual users are targets for ever-more frequent and threatening attacks.

In the 10 years since the Pew Research Center and Elon University's Imagining the Internet Center first asked experts about the future of cyber attacks in 2004 a lot has happened:

- Some suspect the Russian government of attacking or encouraging organized crime assaults on official websites in the nation of Georgia during military struggles in 2008 that resulted in a Russian invasion of Georgia.

- In 2009-2010, suspicions arose that a sophisticated government-created computer worm called "Stuxnet" was loosed in order to disable Iranian nuclear plant centrifuges that could be used for making weapons-grade enriched uranium. Unnamed sources and speculators argued that the governments of the United States and Israel might have designed and spread the worm.

- The American Defense Department has created a Cyber Command structure that builds Internet-enabled defensive and offensive cyber strategies as an integral part of war planning and war making.

- In May, five Chinese military officials were indicted in Western Pennsylvania for computer hacking, espionage and other offenses that were aimed at six US victims, including nuclear power plants, metals and solar products industries. The indictment comes after several years of revelations that Chinese military and other agents have broken into computers at major US corporations and media companies in a bid to steal trade secrets and learn what stories journalists were working on.

- In October, Russian hackers were purportedly discovered to be exploiting a flaw in Microsoft Windows to spy on NATO, the Ukrainian government, and Western businesses.

- The respected Ponemon Institute reported in September that 43% of firms in the United States had experienced a data breach in the past year. Retail breaches, in particular, had grown in size in virulence in the previous year. One of the most chilling breaches was discovered in July at JPMorgan Chase & Co., where information from 76 million households and 7 million small businesses was compromised. Obama Administration

officials have wondered if the breach was in retaliation by the Putin regime in Russia over events in Ukraine.

- Among the types of exploits of individuals in evidence today are stolen national ID numbers, pilfered passwords and payment information, erased online identities, espionage tools that record all online conversations and keystrokes, and even hacks of driverless cars.

- Days before this report was published, Apple's iCloud cloud-based data storage system was the target of a so-called "man-in-the-middle" attack in China that was aimed at stealing users' passwords and spying on their account activities. Some activists and security experts said they suspected the Chinese government had mounted the attack, perhaps because the iPhone 6 had just become available in the country. Others thought the attack was not sophisticated enough to have been government-initiated.

- The threat of cyber attacks on government agencies, businesses, non-profits, and individual users is so pervasive and worrisome that this month (October 2014) is National Cyber Security Awareness Month.

To explore the future of cyber attacks we canvassed thousands of experts and Internet builders to share their predictions. We call this a canvassing because it is not a representative, randomized survey. Its findings emerge from an "opt in" invitation to experts, many of whom play active roles in Internet evolution as technology builders, researchers, managers, policymakers, marketers, and analysts. We also invited comments from those who have made insightful predictions to our previous queries about the future of the Internet. (For more details, please see the section "About this Canvassing.")

Overall, 1,642 respondents weighed in on the following question:

> **Major cyber attacks:** By 2025, will a major cyber attack have caused widespread harm to a nation's security and capacity to defend itself and its people? (By "widespread harm," we mean significant loss of life or property losses/damage/theft at the levels of tens of billions of dollars.)
>
> **Please elaborate on your answer.** (Begin with your name if you are willing to have your comments attributed to you.) Explain what vulnerabilities nations have to their sovereignty in the coming decade and whether major economic enterprises can or cannot thwart determined opponents. Or explain why you

think the level of threat has been hyped and/or why you believe attacks can be successfully thwarted.

Some 61% of these respondents said “yes” that a major attack causing widespread harm would occur by 2025 and 39% said “no.”

Key themes:
Yes, there will be major cyber attacks causing widespread harm

1) Internet-connected systems are inviting targets. The Internet is a critical infrastructure for national defense activities, energy resources, banking/finance, transportation, and essential daily-life pursuits for billions of people. The tools already exist to mount cyber attacks now and they will improve in coming years—but countermeasures will improve, too.

2) Security is generally not the first concern in the design of Internet applications. It seems as if the world will only wake up to these vulnerabilities after catastrophe occurs.

3) Major cyber attacks have already happened, for instance the Stuxnet worm and attacks in nations where mass opposition to a regime has taken to the streets. Similar or worse attacks are a given.

4) Cyber attacks are a looming challenge for businesses and individuals. Certain sectors, such as finance and power systems, are the most vulnerable. There are noteworthy divides between the prepared and the unprepared.

Key themes:
No, there will not be major cyber attacks

1) There is steady progress in security fixes. Despite the Internet's vulnerabilities, a distributed network structure will help thwart the worst attacks. Security standards will be upgraded. The good guys will still be winning the cyber security arms race by 2025.

2) Deterrence works, the threat of retaliation will keep bad actors in check, and some bad actors are satisfied with making only small dents in the system so they can keep mining a preferred vulnerability and not have it closed off.

3) Hype over cyber attacks is an exaggeration of real dangers fostered by the individuals and organizations that will gain the most from creating an atmosphere of fear.

There was little disagreement that the spread and importance of the Internet in the lives of people, businesses, and government agencies exposes them all to new dangers.

As **Jay Cross**, the chief scientist at Internet Time Group, summarized his "yes" answer: "Connectedness begets vulnerability."

Or, as Joel Brenner, the former counsel to the National Security Agency explained in the *Washington Post* this past weekend: "The Internet was not built for security, yet we have made it the backbone of virtually all private-sector and government operations, as well as communications. Pervasive connectivity has brought dramatic gains in productivity and pleasure but has created equally dramatic vulnerabilities. Huge heists of personal information are common, and cybertheft of intellectual property and infrastructure penetrations continue at a frightening pace."

There was considerable agreement among the experts in this canvassing that individuals—their accounts and their identities—will be more vulnerable to cyber attacks from bad actors in the future and that businesses will be persistently under attack. Many said the most vulnerable targets include essential utilities. Many also believe that theft at a larger scale than is now being experienced and economic disruptions could be likely.

The experts had varying opinions about the likely extent of damage and disruption possible at the nation-state level. Many argued that cyber attacks between nations have already occurred, often citing as an example the spread of the Stuxnet worm. The respondents also invoked the Cold War as a metaphor as they anticipated the world to come. They argued that the cyber deterrence of mutually assured disruption or destruction would likely keep competing powers from being too aggressive against other nation-states. At the same time, they also anticipate the current cyber arms race dynamic will expand as nations and other groups and individuals ceaselessly work to overcome security measures through the design of potent exploits.

Some expect that opponents of the political status quo in many regions of the world will work to implement cyber attacks against governments or other entrenched institutions. One "yes" respondent, **Dave Kissoondoyal**, CEO for KMP Global Ltd., put it this way: "I would not say that a major cyber attack will have caused widespread harm to a nation's security and capacity to defend itself and its people, but the risks will be there. By 2025, there will be widespread use of cyber terrorism and countries will spend a lot of money on cyber security."

Some observed that the Internet's expansion will multiply vulnerabilities of all types, even inside one's home. **Tim Kambitsch**, an activist Internet user, wrote, "The Internet of Things is just emerging. In the future, control of physical assets, not just information, will be open to cyber attack."

Some respondents who know the technology world well, but are not privy to insider knowledge about cyber threats, expressed uncertainty about the state of things and whether the disaster scenarios that are commonly discussed are hyped or not. The vice president of research and consumer media for a research and analysis firm observed, "There are serious problems, but it's not clear that those who are directing the hype are focused on the correct problems or solutions. So, the problem is both serious and over-hyped."

Security-oriented experts expressed concerns. **Jeremy Epstein,** a senior computer scientist at SRI International, said, "Damages in the billions will occur to manufacturing and/or utilities but because it ramps up slowly, it will be accepted as just another cost (probably passed on to taxpayers through government rebuilding subsidies and/or environmental damage), and there will be little motivation for the private sector to defend itself. Due to political gridlock and bureaucratic inertia, the government will be unable to defend itself, even if it knows how. The issue is not primarily one of technical capability (although we're sorely lacking in that department). The primary issue is a lack of policy/political/economic incentives and willpower to address the problem."

These are among a number of broad themes threaded through the experts' written elaborations in response to this many-layered issue. This report begins with a summary of key comments in three sections: first, remarks from those that expect a major cyber attack by 2025; second, a summary of the comments of those who disagree; and third, elaborations that go beyond the boundary of the specific question.

Following this initial 25-page summary of the findings, we include three more sections with additional insightful observations segmented in identical fashion.

Themes among those who expect 'yes,' there will be major cyber attacks

'Yes' respondents theme 1) Internet-connected systems are inviting targets. The Internet is a critical infrastructure for national defense activities, energy resources, banking/finance, transportation, and essential daily-life pursuits for billions of people. The tools already exist to mount cyber attacks now and they will improve in coming years—but countermeasures will evolve, too.

Joe Kochan, chief operating officer for US Ignite, a company developing gigabit-ready digital experiences and applications, wrote, "Cyber attacks will become a pillar of warfare and terrorism between now and 2025. So much of a country's infrastructure—commerce, finance, energy, education, health care—will be online, and gaining control of or disrupting a country's online systems will become a critical goal in future conflicts."

Mark Nall, a program manager for NASA, responded, "Current threats include economic transactions, power grid, and air traffic control. This will expand to include others such as self-driving cars, unmanned aerial vehicles, and building infrastructure. In addition to current methods for thwarting opponents, growing use of strong artificial intelligence to monitor and diagnose itself, and other systems will help as well."

Geoff Livingston, author and president of Tenacity5 Media, responded, "Cyberwar is the battlefield of now. Don't kid yourself. Battlefields in Sudan, Afghanistan, and Syria are real, but there is a new battlefield and every day wars are won and lost between individuals, businesses, and countries. The Pentagon and China's military are regularly engaged in digital spats. We really have no idea how deep this goes, but we are much closer to William Gibson's vision in the seminal cyberpunk novel *Neuromancer* than any of us would like to admit."

Herb Lin, chief scientist for the Computer Science and Telecommunications Board at the National Research Council of the US National Academies of Science, replied, "More likely is cyber sabotage of individual enterprises. On a large scale, cyber attacks may be combined with kinetic attacks and the combination may cause large-scale damage."

Christian Huitema, a distinguished engineer with Microsoft, observed, "We are already witnessing the theft of trade secrets, with impact well worth tens of billions of dollars. We are also seeing active development of cyber weapons by many world powers. Historically, such new weapons are always used at least once or twice before nations realize it is too dangerous and start relying on diplomacy."

Stewart Baker, a partner at Steptoe & Johnson, a Washington law firm, wrote, "Cyberwar just plain makes sense. Attacking the power grid or other industrial control systems is asymmetrical and deniable and devilishly effective. Plus, it gets easier every year. We used to worry about Russia and China taking down our infrastructure. Now we have to worry about Iran and Syria and North Korea. Next up: Hezbollah and Anonymous."

Lee McKnight, a professor of entrepreneurship and innovation at the Syracuse University's School of Information Studies, said, "Cyber security extortionists just made $100 million in 60 days (see 'Cryptolocker'). So on one hand it is easy to extrapolate and imagine significant harm done to individual users and institutions given the black hats' upper hand in attacking systemic vulnerabilities, to the extent of tens of billions in financial losses; and in loss of life. But security systems are progressing as well; the white hat good guys will not stop either. While inter-connected digital systems will be far more pervasive in 2025, they will still be, largely, amalgams of not fully automated and interconnected systems, which also provides a degree of insulation against national cyber attacks causing the degree of harm to people and property imagined by this question. While in principle all systems are crackable, it is also possible to embed security far more deeply in the Future Internet than it is in the present Internet environment. Obviously it is in the interest of the cyber security industrial complex and its participating firms to hype threats. On the other hand, a great deal of critical infrastructure is very vulnerable to cyber and physical attack. Imagining bad scenarios where those facts intersect is worrisome, but I remain optimistic the good guys will keep winning; in general."

'Yes' respondents theme 2) Security is generally not the first concern in the design of Internet applications. It seems as if the world will only wake up to these vulnerabilities after catastrophe occurs.

Patrick Tucker, futurist and author of *The Naked Future: What Happens In a World That Anticipates Your Every Move?* said, "Today, cities around the world use supervisory control and data acquisition (SCADA) systems to manage water, sewage, electricity, and even traffic lights. Independent analysis has found that these systems suffer from 25 different security vulnerabilities. That's bad enough, but then consider how human error and incompetence makes these common systems even less secure. Many of the IT managers that use these systems haven't changed the manufacturer-installed security codes. As writers Indu B. Singh and Joseph N. Pelton have pointed out in The Futurist magazine, that failure to take even the most basic security precautions leaves these systems open to remote hacking."

Stuart Umpleby, a systems theory expert and professor at George Washington University wrote, "In addition to cyber attacks there are threats from individuals who have access (e.g., Manning,

Snowden, Bernie Madoff, Steven Cohen). Digital equipment is vulnerable to solar flares and EMP (electromagnetic pulse). There can be overlooked or underestimated design flaws (e.g., the Y2K bug, Long Term Capital Management, financial derivatives, or the change in the Glass-Steagall Act). Possible solutions: 1. Decentralization can stop cascade effects. However, decentralization plus connection can lead to vulnerabilities since no one is in charge. 2. Oversight and regulation. However, technical regulation requires highly skilled people and the private sector pays higher salaries. Firms also try to keep secrets. In finance the banks are now in a position to write the rules that regulate them. Big banks are getting bigger. So far losses in the billions have been due to financial and political design flaws more than technical design flaws."

Elena Kvochko, manager for IT industry at an international organization based in New York, noted, "The possibility of a widespread cyber attack on national critical infrastructure is a major concern for many governments. The scope and the consequences of such attacks may be different for different nations. However, a large portion of critical infrastructure facilities still rely on software and technology created decades ago and which has not been upgraded. The level of sophistication of adversaries generally progresses much faster, therefore, it is important to implement adequate measures to ensure a proper protection of critical assets and capabilities."

An executive for a major national news organization in the US wrote, "The government and the private sector are responding too slowly to this threat. We've already seen the US Chamber of Commerce hacked, allegedly by the Chinese. We've seen numerous 'botnet' attacks on financial institutions that have rendered their sites unusable for hours at a time. And, at the moment, there's little political will to impose minimal cybersecurity standards even on 'essential' businesses, such as electric utilities, telecommunications companies and financial institutions. Some Obama administration officials have warned of a coming 'Cyber Pearl Harbor.' Still, the public and many businesses seem sanguine about this possibility."

Ben Fuller, dean of humanities and sustainable development at the International University of Management in Windhoek, Namibia, responded, "A major vulnerability lies in the capacity of nations and businesses to understand cyber threats and to take prudent preventative steps. For example, I am involved in the administration of .NA here in Namibia. A few years ago we were one of the first ccTLDs worldwide to implement Internet Domain Name System Security (DNSSEC). DNSSEC is an important security protocol for Domain Name System operations. Implementing DNSSEC is neither complicated nor prohibitively expensive. Namibia, despite its apartheid past, has grown into an upper-middle-income country according to the World Bank, hence our economy depends heavily on the Internet—the banking, financial, mining, transport, and tourism sectors in particular. Yet, local interest in adopting DNSSEC has been disappointing. This is one instance

where network administrators are not taking advantage of existing tools to improve network security. One wonders if our experience with DNSSEC represents a larger pattern."

Vanda Scartezini, a partner in Polo Consultores Associados, based in Brazil, replied, "I do believe one or two major attacks—attacking critical infrastructure such as general utilities like electricity or water, with huge consequences on day-to-day life—will happen until the real efforts on cyber security come to a common agreement among all nations. I believe it will happen in a small, developing country first and then a more relevant country will be the target and the impact will bring all parties to the table of negotiation followed by the action needed."

'Yes' respondents theme 3) Major cyber attacks have already happened, for instance the Stuxnet worm and attacks in nations where mass opposition to a regime has taken to the streets. Similar or worse attacks are a given.

A notable number of respondents cited Stuxnet and other acts against various populations as evidence that cyber attacks were now integrated into national military and intelligence strategies.

The Stuxnet computer worm, according to a publication of the Institute of Electrical and Electronics Engineers, infected the software of at least 14 industrial sites in Iran several years ago. A worm is not like a computer virus, which must be installed—unwittingly—by a user in order to work. Instead, a worm spreads on its own among computers once it has been introduced to a network. In the case of Stuxnet the worm targeted computer systems tied to production of Iran's nuclear program and helped destroy as many as a fifth of the centrifuges.

Jason Pontin, editor in chief and publisher of MIT Technology Review, wrote, "Oh, sure it is possible. Although not at your defined level, there has already been a 'Pearl Harbor' event: the Stuxnet computer worm that was used to attack Iran's nuclear capabilities. Do we really believe that the infrastructure of a major industrial power will not be so attacked in the next twelve years? The Internet is an insecure network; all industrialized nations depend on it. They're wide open."

Stowe Boyd, lead researcher for GigaOM Research, said, "A bellicose China might 'cyber invade' the military capabilities of Japan and South Korea as part of the conflict around the China Sea, leading to the need to reconfigure their electronics, at huge cost. Israel and the United States have already created the Stuxnet computer worm to damage Iran's nuclear refinement centrifuges, for example. Imagine a world dependent on robotic farm vehicles, delivery drones, and AI-managed transport, and how one country might opt to disrupt the spring harvest as a means to damage a neighboring opponent."

Judith Perrolle, a professor at Northeastern University in Boston, wrote, “The US government's series of cyber attacks on citizens, economic entities, and governments around the world has already done this. People have died from faulty equipment producing gas pipeline explosions and from drone bombings of civilians. US companies have lost billions worth of business as foreign customers no longer trust their products and services. One way to counter such attacks is by diplomacy and respect for international law, especially by the United States. As one of my students once titled a paper on Stuxnet: ‘People who live in electronic houses shouldn't throw worms.’ A second line of defense is to design computer and information systems to be more secure. Our current systems are incredibly vulnerable, by design. US cyber security efforts seem dedicated to breaking into computer systems, not securing them.”

Maurice Vergeer, an assistant professor at Radboud University Nijmegen in the Netherlands, replied, “It probably will. Estonia was one of the first countries that suffered a major cyber attack some years ago. If an agency can create something like Stuxnet to sabotage Iranian nuclear facilities, it's a question of time for another agency to come up with another piece of malware to sabotage essential infrastructure. The problem is that because of the Internet of things, this is even more likely because most computers and machines will be connected to the Internet. Even when security is tight, the human factor is probably the weakest link.”

‘Yes’ respondents theme 4) Cyber attacks are a looming challenge for businesses and individuals. Certain sectors, such as finance and power systems, are the most vulnerable. There are noteworthy divides between the prepared and the unprepared.

Henning Schulzrinne, Internet Hall of Fame member and a technology developer and professor at Columbia University, said, “Primarily financial services (both trading and financial transactions) and maybe the power grid seem vulnerable and their disruption is most likely to inflict large collateral damage. Both are dominated by legacy systems, with a limited willingness to make the necessary investments in upgrades and, particularly for utilities, limited technical depth in their staff.”

Jim Warren, longtime online freedom and privacy advocate and editor/publisher of microcomputer periodicals, responded, "It seems likely that there will be far more cyber-attacks for the purpose of theft and/or economic harm to their targets, than for the purpose of causing physical harm to individuals or groups.”

Tim Bray, an active participant in the IETF and technology industry veteran, made this basic point, even though he answered “no” to the overall question: “I'm sure there will be devastating

economic attacks against companies, sectors, and perhaps whole economies, mostly executed by criminals for gain. But I don't anticipate much in the way of successful state versus state attacks."

Mike Roberts, Internet pioneer and former CEO with ICANN and longtime Internet Society leader, responded, "The distributed 'network of networks' architecture protects us from a concerted attack that brings down major sections of the Net. Having said that, businesses are forced to spend sums they never imagined in order to protect their ability to provide goods and services over the Net, and governments are discovering they can't fake a commitment to security for their own facilities. The Obamacare server fiasco is just one of the more visible examples of politicians believing their own hype about the Net. There ought to be a highly regarded annual award for 'demonstrated Internet security competence.'"

An employee of the Network Information Center observed, "The biggest vulnerabilities are with the financial, energy, and transportation sectors—which represent the soft underbelly of our society and are increasingly under siege from thwarted cyber attacks. In the end, I believe we can keep opponents at bay, but it will require a significantly larger investment by government and industry and the cyber security industry will become a significantly larger employer as a result."

Ray Schroeder, associate vice chancellor for online learning at the University of Illinois-Springfield, wrote, "I fear a cyber attack that will bring down key parts of the national infrastructure and severely damage the economy. I do not expect the Internet itself to suffer irreparable harm. But through the Internet, such infrastructures as the power grid; water and sewage services; hard-wired telephone and cell phone networks may be impaired. These, in turn, would put enormous pressures on the economy and alternative service models. Daily, there are thousands of attacks that are thwarted. But, it is only a matter of time before a large-scale attack succeeds. The key will be to establish effective models for recovery and support."

Themes among those who responded 'no,' there will not be major cyber attacks

'No' respondents theme 1) There is steady progress in security fixes. Despite the Internet's vulnerabilities, a distributed network structure will help thwart the worst attacks. Security standards will be upgraded. The good guys will still be winning the cyber security arms race by 2025.

Bill Woodcock, executive director for the Packet Clearing House, responded, "Not unless there's significant inflation between now and then. Direct losses associated with cyber attacks are always difficult to calculate and attribute. Indirect and intangible losses from large attacks may easily top tens of billions of today's dollars, or even relative value accounting for enlargement of the economy

between now and then. We're at least 25 years into cyber attacks now, and although they get larger, and the economy and population becomes more dependent upon the resources that are vulnerable to them, they still don't have the effect on physical assets and infrastructure that doomsday-predictors have always worried they would. I'm not sure that problem will get worse as people become more sophisticated. I think we're already over that hump."

Glenn Edens, director of research in networking, security, and distributed systems within the Computer Science Laboratory at PARC, a Xerox Company, responded, "Maybe I'm being optimistic but there is steady progress in security. Again, the basic architecture of the Internet is wrong on so many levels—so much needs to be fixed. The loss of financial gains is more likely than a loss of life."

Isaac Mao, chief architect of Sharism Lab, said, "New security standards will help out."

Paul Jones, a professor at the University of North Carolina and founder of ibiblio.org, responded, "Nations and others who hold necessarily secure information are getting better and better about protecting their essential assets. Yes, a bunch of credit card numbers and some personal information will leak. Yes, you may not be able to place an order for a few hours. But it's less and less likely that say all pacemakers in a major city will stop at once or that cyber attacks will cause travel fatalities. I expect increased tension between individual needs, commercial needs, and national needs for privacy, mobility, and security. TOR [anonymizing software] everywhere? Perhaps."

Karl Fogel, a partner with Open Tech Strategies and president of QuestionCopyright.org, said, "Most physical systems that have digital controls are complex enough, and have enough manual intervention built in, that a cyber-attack is just a problem to be dealt with rather than a catastrophe that causes a loss of power grid, airplane crashes, driverless car crashes, water supply poisoning, trains trapped in tunnels, etc. We already have such systems in many places, and there have not been cyber attacks that carry over directly into the physical realm with major consequences. I wouldn't expect engineering principles to be significantly different by 2025."

Robert Bell, of IntelligentCommunity.org, responded, "While the possibility of such widespread disruption certainly exists, it has become a priority among most industrialized nations to understand and respond to the threat. I expect smaller-scale incidents but not large-scale loss of life or billions of dollars of property loss."

Ebenezer Baldwin Bowles, founder and managing editor of CornDancer.com, replied, "Cyber attacks a decade hence shall remain a nuisance but not a foundational threat to a mature nation-

state or a fully funded transnational corporation—always costly per annum to defend against and mitigate after the fact, but never the gateway to an apocalypse. The Internet is too vast, too dynamic, too widely distributed, and too resilient to ever fall prey to an online assault by terrorist cells, cyber gangs, lone geniuses, or hostile military units. The Internet is vulnerable to 'widespread harm' only through direct and massive munitions-based attacks on significant nodes of the physical infrastructure—server farms, electrical grids, energy distribution systems. Determined online opponents are limited by the fundamental underlying structure of the Internet."

'No' respondents theme 2) Deterrence works, the threat of retaliation will keep bad actors in check, and some bad actors are satisfied with making only small dents in the system so they can keep mining a preferred vulnerability and not have it closed off.

David Clark, a senior research scientist at MIT's Computer Science and Artificial Intelligence Laboratory, noted, "The nation-states with the capability to deliver such an attack do not have the motivation to do so. While there will be some actors (e.g., terrorist organizations) that might have the motivation, they currently do not have the skills, and there are easier ways to cause this sort of damage. However, the odds of this outcome are not zero, only low in my view."

Fred Hapgood, a science and technology writer, responded, "On this level, the tens of billions of dollars mark, the risk is very low. A loss on this level will trigger serious retaliation and the hackers responsible can never be 100% certain that they haven't left a trail somewhere. So they will wait for the worst case, and the worst case will probably not arise. Maybe in the context of a shooting war. The stakes would have to be very high."

Garland McCoy, president and founder of the Technology Education Institute, said, "Mutually-assured destruction worked then, works now, and will work in cyberspace."

Bob Briscoe, chief researcher in networking and infrastructure for British Telecom, wrote, "There will have been major cyber attacks, but they are less likely to have caused widespread harm. They will be stealth attacks to extract information and exploit it for commercial and political gain. Harm to an enemy is only a desire of less-sophisticated individuals. Anyone who amasses the ability to mount a major cyber attack, better than their opponent, also doesn't want to lose their position of advantage. They are likely to shift to strategies of gain for their own position, rather than explicit harm to their victim, which would alert their victim and close off their channels of attack, and set back their advantageous position."

Justin Reich, a fellow at Harvard University's Berkman Center for Internet & Society, responded "yes" to the question, but said, "The potential of threat is as real as the potential of nuclear annihilation. It hasn't happened because mutually-assured destruction works, or at least it has for 70 years. We will have this constant, relatively low-grade probing, piracy, and state-sponsored cyber-terrorism."

Todd Cotts, a business professional, wrote, "Cyber attacks will always be a threat, but it is unlikely that a future cyber attack causing widespread harm will occur, any more than today. Cyber warfare is real and will continue to be a growing threat. However, just as the United States has historically been the leader in military advances in the physical world, it will do so in the cyber world, and, as we all know, [such warfare] has been underway for decades now. The challenge will be in whether or not the government is capable of staying ahead of the cyber terrorists. As long as the government leans on a competitive marketplace of non-government companies specializing in technological advances in cyber security, the advances should keep the United States at par, at minimum, with advances by cyber terrorists. The reality is that the more we rely on cyber technologies for automation, communication, controls, security, etc., the more susceptible we are to crippling cyber attacks. Greater concern should be given to the other methods of warfare more likely to cause 'widespread harm': Nuclear being at the top of the list, followed by EMP [Electro-Magnetic Pulse]."

'No' respondents theme 3) Hype over cyber attacks is an exaggeration of real dangers fostered by the individuals and organizations that will gain the most from creating an atmosphere of fear.

Jonathan Grudin, principal researcher at Microsoft Research, responded, "Perhaps I am optimistic, but this concern seems exaggerated by the political and commercial interests that benefit from us directing massive resources to those who offer themselves as our protectors. It is also exaggerated by the media because it is a dramatic story. President Eisenhower worried that we would suffer if we had leaders who would not rein in the military-industrial complex, and it is clear our leaders are powerless to rein in the military-industrial-intelligence complex, whose interests are served by having us fearful of cyber attacks. Obviously there will be some theft and perhaps someone can exaggerate it to claim tens of billions in losses, but I don't expect anything dramatic and certainly don't want to live in fear of it."

Mike Caprio, a software engineer for a consulting firm, wrote, "Cyber attacks are a boondoggle invented by military-industrial contractors to bilk governments out of billions of dollars. The infrastructure is not as fragile or attackable as they would claim."

Kelly Baltzell, CEO for Beyond Indigo, wrote, "I believe cyber attacks do happen but think the threat level is completely hyped. Fear makes people cringe and not employ their own internal power and common sense. Right now with the NSA issues and such, we are finding out that the major countries are already spying, hacking, and causing problems. The use of the term 'for national security' invokes people to panic, fear, and give up the privacy they do have in exchange for what they think is safety. People just need to be rational and realize that other people in other countries just want to live, raise their families, and enjoy life. It takes a lot of energy to hate and create negativity on an ongoing basis."

Above-and-Beyond Responses: Part 1

A variety of views in regard to this issue are reflected in these big thinkers' imaginings of what may happen by 2025.

Look for losses in intellectual property and via 'data pollution'

Vint Cerf, Google vice president and co-inventor of the Internet Protocol, responded, "Yes, while it has been predicted for a long time, there is no question that intellectual property theft is an increasingly serious problem and the potential hazard of data pollution looms. Estonia is the prototypical example. A lot will have been done by 2025 to increase security and safety online but there will still be exploitable vulnerabilities. Systems that observe their own behavior and the behavior of users may be able to detect anomalies and attacks. There may well be some serious damage in the financial sector especially (identity theft is still a problem, etc.). The use of things like Bitcoin, if prevalent, will produce wildly gyrating values and high risks."

Many attacks will have a 'cyber add-on' component

Jamais Cascio, a writer and futurist specializing in possible futures scenario outcomes, wrote, "Depending upon how it's understood, this could also be a 'yes' or 'no' answer. We'll likely see a major attack that has a cyber component, but less likely to see a major cyber-only attack. In this cyber-add-on scenario, other forms of attack (from simple bombing to infrastructure damage to bioweapons) are enhanced by digital or electronic assaults meant to hamper our ability to recognize and respond to the main thrust of the attack. Cyber is a force-multiplier, in strategic terms, but not necessarily a useful solo vector. Here's why: hitting a system large enough and pervasive enough that its loss will have major, widespread harmful consequences would take an extraordinary combination of time, coordination, sophistication and luck. Networked systems already exist in a hostile environment, and attention/resources are already being directed to system security—there's a greater likelihood of a complex assault being spotted. Furthermore, redundancy, backups, and ready alternatives can mitigate the harm of a cyber infrastructure attack, and it's hard to say from simple observation, which systems will be or won't be supported in this way. This doesn't make a sophisticated attack impossible by any means, but it makes such an attack much more difficult, and the results less certain. A hostile actor will want greater certainty of outcome and less of a potential to be caught. A cyber-only attack is possible, but less efficient (and likely less effective) than simpler attacks."

'Collaboration and cooperation' among all parties are essential

Amy Webb, digital media futurist and founder of Webbmedia Group, wrote, "It's quite possible. One big challenge is that in the digital space, typical geographic boundaries don't apply. If you

have a credit card, that company is likely using Amazon Web Services with servers in multiple countries. Amazon protects itself, but individual countries establish laws describing what constitutes a crime and how cybercrime will be punished. There is no overarching law that rules everyone, and some culturally different activities are more accepted than others. Likewise, depending on the person, her knowledge, and where she lives in the world, she may regularly pass along security bugs and viruses that could, along with many other users, contribute to a widespread outage. In order for us all to be safe and protected, collaboration and cooperation among governments, businesses, and individuals is necessary."

Jeff Jarvis, director of the Tow-Knight Center for Entrepreneurial Journalism at the City University of New York Graduate School of Journalism, wrote, "There will be continuing attacks bringing continuing damage. The question is how big an industry that will spawn in securing systems against such danger and mitigating risk. But security comes not only from government and industry. It also comes from the huge forces of collaboration and volunteerism that can coalesce around open source as a means of assuring that many eyes will watch for vulnerabilities and many hands will fix the faults that are found."

'Far too much of the world's computing capacity is defenseless'

Jerry Michalski, founder of REX, the Relationship Economy eXpedition, wrote, "A tremendous proportion of the devices on the Net—personal computers as well as devices—have been compromised already, or will be compromised in the near future. Any device that isn't attended to regularly to keep it from being vulnerable should be written off as part of the darknet. Targeted attacks should rise, as should dysfunctional ideas (memes), spread to sew discord or doubt. Far too much of the world's computing capacity is defenseless. Anything with firmware that can't be upgraded securely in the field is vulnerable. Loss of life may be more difficult than loss of property, as property becomes ones and zeroes. National boundaries will matter less and less, despite countries' attempts to secure those boundaries and control their populations. People will join 'nations of choice,' giving their allegiance to loose organizations that have principles they love, such as Burning Man, the Tea Party, Occupy, and others that will emerge in the next few years."

We must adjust our obsession with efficiency to also focus on 'resilience'

David Brin, author and futurist, wrote, "We must move from the 1990s obsession with 'efficient' production—e.g., just-in-time manufacturing. That proved disastrous after Fukushima. In nature, resilience is just as important as efficiency. If we work on it, our resilience will make a crucial difference making such attacks futile."

Natural disasters cause more devastation

Hal Varian, chief economist for Google, predicted, "There will certainly continue to be cyber attacks around the world. However, I don't think that such attacks will involve losses of tens of billions of dollars. For that to happen we would have to see systems down for several days. Katrina was the costliest US hurricane and it did about $100 billion of damages. Most hurricanes have been in the $20 billion range. I don't see cyber attacks coming anywhere close to hurricanes in terms of the associated property losses."

Security awareness and actions 'will become a necessary part of life'

Jim Hendler, a professor of Computer Science at Rensselaer Polytechnic Institute, wrote, "I don't believe a single major cyber attack of this kind will be a key event, rather there will be a growing number of smaller attacks and crime which cause increased awareness and willingness of people to take better cyber security—security online will become a necessary part of life, varying by where in cyberspace one is—much the way home security or car security is today."

The worst events might be caused by accident

Joel Halpern, a distinguished engineer at Ericsson, wrote, "Any response to this is very much a guess, as what will happen depends both on what can happen and on what people choose to do. I would not be surprised if there was a network-based event which caused tens of billions of dollars in damage. I would expect that it is more likely to occur by accident than it is by deliberate action. This is based on the observation that random coincidental failures are much harder to plan for than human intention."

'On balance, it is a nail-biter'

Paul Saffo, managing director at Discern Analytics and consulting associate professor at Stanford University, replied, "The question is missing the button I wanted to push: 'Maybe.' This is a classic wild-card issue: uncertain probability but potentially enormous impact. We will certainly have a steadily increasing number of cyber attacks by both state and non-state actors. The uncertain part is the scale of effects, and that is time-dependent: there is a race on between cyber defense tools and cyberattack capability, and at any given moment, one is slightly ahead of the other. On balance, it is a nail-biter. It is a close call, but I think we will have a bunch of scares, but will squeak through. More generally, my fear is that we are neglecting the risk of 'cyber errors' in creating wild disruptions. Stupidity is always more common than evil."

Look for cyber treaties before things get too far out of hand

Fred Baker, Internet pioneer, longtime leader in the IETF and Cisco Systems Fellow, responded, "This is a little like asking whether the existence of a nuclear arsenal implies the eventuality of nuclear attack. I do believe that it is possible to perpetrate such attacks now, and we have seen tete-a-tete between nation-state actors in Eastern Europe, the Middle East, Asia, and North America. However, the perpetration of an attack that causes 'significant loss of life or property losses/damage/theft at the levels of tens of billions of dollars' is likely to draw a comparable retaliation, and like the outcomes of nuclear assault, become its own counter-measure. It may, like nuclear arsenals, become a matter of treaty discussion."

The digital 'immune system' will respond

Seth Finkelstein, a programmer, consultant and EFF Pioneer of the Electronic Frontier Award winner, wrote, "In general, for critical infrastructure, I'd say there's enough low-level threat from ongoing minor attacks to make it difficult to pull off a really major attack. Much of this entwines with credit card security. Grabbing a bunch of credit card numbers is both far more profitable and far easier to do than massive disruption. So defending against that type of ongoing crime is sort of like an immune system challenge that helps guard against even more harmful attacks."

Fixing privacy problems will also make things more secure

Marcel Bullinga, a futurist and trend watcher, predicted, "The answer is connected to the privacy-enhanced infrastructure. If you have accomplished that, you have a safe infrastructure as well, not so vulnerable to cyber attacks. I guess a wildcard will do the trick of speeding up the creation of a safe infrastructure—the explosion of a nuclear reactor or the theft of $200 billion in one second caused by a cyber attack."

There will be a large-scale manipulation of the Web but 'we will overcome it.'

Tiffany Shlain, filmmaker, host of the AOL series *The Future Starts Here* and founder of The Webby Awards, observed, "There will be attacks, but just as quickly as they happen, we will figure out how to combat them. The Web is merely an extension of us as humans. We are good and bad and everything in between. But ultimately, I believe we are good. The Web will at some point have large-scale manipulation with malicious intent, but we will learn from it and overcome it."

> **Doc Searls**, director of ProjectVRM at Harvard University's Berkman Center for Internet & Society, wrote at length on this issue:
>
> "I imagine that Iran would already claim that it has suffered harm through the (alleged but

widely acknowledged) Stuxnet attack by the US and Israel on Iranian nuclear facilities. No doubt other forms of cyber warfare are ready for deployment by the U.S., Russia, China and other countries. Since what can be done will be done, sooner or later, it is reasonable to expect harm in $billions (at current valuation)—to some country, or number of countries. On the other hand, the whole world is now one big system, and it will be very hard to contain the effects of a cyber attack, as we discovered (predictably) with Stuxnet.

Two questions need to be asked: 1) Who in a country is most capable of cyber-warfare? Is it the government or the hackers? 2) Is it in the national interest of a country to attack another with which it enjoys a high degree of business and other dealings? In business today, many old enemies are now close friends, at least in business.

In Russia today the concentration of techno-experts making money through botnets off of the (mostly U.S.-based) $many-billion advertising industry is very high. Is there a higher concentration of experts inside the Russian government? Almost certainly not, given the billions being made in Russia's clandestine botnet business.

My point here is that actors in the private sector, especially the bad-guy ones, may have stronger cyber warfare skills than their own governments. And they are already doing damage in the form of many billions of dollars siphoned off the flow of advertising money through Google and other companies.

What happens when the online advertising business, which has many characteristics of mania and bubble, starts to fail? If one doubts that failure will happen, consider this: more than 61% of traffic on the Net already isn't human, and a third of that number is busy impersonating human traffic, no doubt for fraudulent purposes. Also, according to Michael Tiffany of White Ops, 'at least 15 percent of American broadband households are participating in a botnet right now.' And the numbers are going up.

"Both cryptography and cracking it continue to get more sophisticated. Those who are good at it won't stop. And all the countries capable of cyber warfare—China, the US, Russia, India, the UK, Israel and so on—are not going to stop preparing for it and doing everything they can to stay ahead of both their friends and their enemies, real and perceived. This constitutes a cold war of sorts. Likewise, spying also won't end. Spy agencies will do what they were created to do. They have always been, by nature and charter, outside the laws of both their own countries and those they spy on.

So we have this broad class of things we know—notably the level of cyber crime happening constantly, and its effects on the whole Internet—and a narrow class of things we don't, which is what the spy agencies know but won't say. (Yes, Snowdens come along from time to time, but the spying will continue.)

To sum up, I believe we can safely predict that cyber crime will be one of the daggers that burst the online advertising bubble, the collapse of which will cause harm to some industries (e.g., online publishing). But all bets are off for what will happen in cyber warfare. The one clear thing is that national boundaries and interests are far more blurred than they ever were when wars happened in the physical world alone."

About this Canvassing of Experts

The expert predictions reported here about the impact of the Internet over the next 10 years came in response to one of eight questions asked by the Pew Research Center Internet Project and Elon University's Imagining the Internet Center in an online canvassing conducted between November 25, 2013, and January 13, 2014. This is the sixth Internet study the two organizations have conducted together since 2004. For this project, we invited more than 12,000 experts and members of the interested public to share their opinions on the likely future of the Internet and 2,551 responded to at least one of the questions we asked. Some 1,642 responded to this question about cyber attacks.

The Web-based instrument was fielded to three audiences. The first was a list of targeted experts identified and accumulated by Pew Research and Elon University during the five previous rounds of this study, as well as those identified across 12 years of studying the Internet realm during its formative years. The second wave of solicitation was targeted to prominent listservs of Internet analysts, including lists titled: Association of Internet Researchers, Internet Rights and Principles, Liberation Technology, American Political Science Association, Cybertelecom, and the Communication and Information Technologies section of the American Sociological Association. The third audience was the mailing list of the Pew Research Center Internet Project, which includes those who closely follow technology trends, data, and themselves are often builders of parts of the online world. While most people who responded live in North America, people from across the world were invited to participate.

Respondents gave their answers to the following prompts:

> **Major cyber attacks:** By 2025, will a major cyber attack have caused widespread harm to a nation's security and capacity to defend itself and its people? (By "widespread harm," we mean significant loss of life or property losses/damage/theft at the levels of tens of billions of dollars.)
>
> **Please elaborate on your answer.** (Begin with your name if you are willing to have your comments attributed to you.) Explain what vulnerabilities nations have to their sovereignty in the coming decade and whether major economic enterprises can or cannot thwart determined opponents. Or explain why you think the level of threat has been hyped and/or why you believe attacks can be successfully thwarted.

Since the data are based on a non-random sample, the results are not projectable to any population other than the individuals expressing their points of view in this sample. The respondents' remarks reflect their personal positions and are not the positions of their employers; the descriptions of their leadership roles help identify their background and the locus of their expertise. About 84% of respondents identified themselves as being based in North America; the others hail from all corners of the world. When asked about their "primary area of Internet interest," 19% identified themselves as research scientists; 9% said they were entrepreneurs or business leaders; 10% as authors, editors or journalists; 8% as technology developers or administrators; 8% as advocates or activist users; 7% said they were futurists or consultants; 2% as legislators, politicians or lawyers; 2% as pioneers or originators; and 33% specified their primary area of interest as "other."

On this particular question many of the respondents elected to remain anonymous. Because people's level of expertise is an important element of their participation in the conversation, anonymous respondents were given the opportunity to share a description of their Internet expertise or background.

Here are some of the key respondents in this report:

Miguel Alcaine, International Telecommunication Union area representative for Central America; **Jari Arkko**, chair of the Internet Engineering Task Force; **Francois-Dominique Armingaud**, formerly a computer engineer for IBM now teaching security; **Stowe Boyd**, lead at GigaOM Research; **Bob Briscoe**, chief researcher for British Telecom; **Vint Cerf**, vice president and chief Internet evangelist at Google; **David Clark**, senior scientist at MIT's Computer Science and Artificial Intelligence Laboratory; **Glenn Edens**, research scientist at PARC and IETF area chair; **Jeremy Epstein**, a senior computer scientist at SRI International; **Seth Finkelstein**, a programmer, consultant and EFF Pioneer of the Electronic Frontier Award winner; **Jonathan Grudin**, principal researcher for Microsoft; **Joel Halpern** a distinguished engineer at Ericsson; **Jim Hendler**, Semantic Web scientist and professor at Rensselaer Polytechnic Institute; **Christian Huitema**, distinguished engineer with Microsoft; **Jeff Jarvis**, director of the Tow-Knight Center at the City University of New York; **Clifford Lynch**, executive director of the Coalition for Networked Informatin; **Jerry Michalski**, founder of REX, the Relationship Economy eXpedition; **Ian Peter**, pioneer Internet activist and Internet rights advocate; **Raymond Plzak**, former CEO of the American Registry for Internet Numbers, now a member of the board of ICANN; **Jason Pontin**, editor in chief and publisher of MIT Technology Review; **Mike Roberts**, Internet Hall of Famer and longtime leader with ICANN; **Paul Saffo**, managing director of Discern Analytics and consulting associate professor at Stanford; **Barbara Simons**, former president of ACM and board chair for Verified Voting; **Doc Searls**, director of

ProjectVRM at Harvard's Berkman Center; **Stuart Umpleby**, systems theory expert and professor at George Washington University; and **Hal Varian**, chief economist for Google.

Here is a selection of other institutions at which respondents work or have affiliations:

Yahoo; Intel; IBM; Hewlett-Packard; Nokia; Amazon; Netflix; Verizon; PayPal; BBN; Comcast; US Congress; EFF; W3C; The Web Foundation; NASA; Association of Internet Researchers; Bloomberg News; World Future Society; ACM; the Aspen Institute; GigaOm; the Markle Foundation; the Network Information Center; key offices of US and European Union governments; the Internet Engineering Task Force; the Internet Hall of Fame; ARIN; Nominet; Oxford Internet Institute; Princeton, Yale, Brown, Georgetown, Carnegie-Mellon, Duke, Purdue, Florida State and Columbia universities; the universities of Pennsylvania, California-Berkeley, Southern California, North Carolina-Chapel Hill, Kentucky, Maryland, Kansas, Texas-Austin, Illinois-Urbana-Champaign, the Georgia Institute of Technology, and Boston College.

Complete sets of credited and anonymous responses to this question, featuring many dozens of additional opinions, can be found on the Imagining the Internet site:

http://www.elon.edu/e-web/imagining/surveys/2014_survey/2025_Internet_Cyber_Attacks.xhtml
http://www.elon.edu/e-web/imagining/surveys/2014_survey/2025_Internet_Cyber_Attacks_credit.xhtml
http://www.elon.edu/e-web/imagining/surveys/2014_survey/2025_Internet_Cyber_Attacks_anon.xhtml

Elaborations: More Expert Responses

Following are additional provocative and thoughtful answers from other respondents, organized in the same format as those in the summary. First, the insights of those who responded "yes" to the question, next the thoughts of those who answered "no," closing with additional observations.

Themes among those who responded 'yes,' there will be major cyber attacks

'Yes' respondents theme 1) Internet-connected systems are inviting targets. The Internet is a critical infrastructure for national defense activities, energy resources, banking/finance, transportation, and essential daily-life pursuits for billions of people. The tools already exist to mount cyber attacks now and they will improve in coming years—but countermeasures will improve, too.

Robert E. McGrath, an Internet pioneer and software engineer who participated in developing the World Wide Web and advanced interfaces, replied, "Cyber attacks are already pervasive, and it is trivial even for children to acquire the means to inflict serious damage. The United States has already attacked other countries, and other deliberate attacks are suspected. Losses are already in the tens of billions. 'National sovereignty' is pretty meaningless on the Internet anyway, so I can't say anything about it. It is only a matter of time before there is a serious incident, i.e., one that journalists recognize as an event."

John E. Savage, chair in computer science at Brown University and a fellow of the IEEE, and the ACM, wrote, "The integration of national critical infrastructures such as the electrical grid, the financial industry, and corporations into the Internet has created a system that is more fragile than is generally recognized. Computer security in these systems has been and is very weak. While it is unlikely that any one major nation is likely to try to damage the critical infrastructure of another given the potential for blowback, accidents and misunderstandings are a serious possibility. An example of this is the aggressive posture of China vis-a-vis its surrounding waters. They have claimed control over the entire South China Sea through which 25 percent of the world's maritime shipping occurs and now are claiming sovereignty over a large portion of the East China Sea. If tensions rise over their assertions and an accident occurs at the same time that shuts off the electricity in a large portion of the United States and malware attributed to China is found within computers controlling the electric grid, escalation and further damage are likely. The undersea cable system carries more than 95% of the global Internet traffic. This includes at least $10 billion in financial transactions per day. Damage to a large portion of this system lasting days or weeks could easily reach the threshold cited in the question. The Federal Bank of Boston

handles more than $4 billion in transactions per day for the Federal Reserve. If its systems were damaged, the threshold could be reached in a few days."

Mikey O'Connor, an elected representative to the GNSO Council of ICANN, representing the ISP and connectivity provider constituency, said, "Cyber infrastructure constantly teeters on the edge of collapse. However, the odds of a 'successful' cyber attack causing extreme harm continue to rise—to almost-certainty between now and 2025—as attackers shift from individuals with limited resources to state-funded warriors. The severity and breadth of harm that can be caused also continues to rise as dependence on cyber-resources increases. Similarly, developing countries will become more vulnerable as they ramp up their Internet capability and dependence."

Jeff Jaffe, the CEO for the World Wide Web Consortium, the standards-setting body for the Web, wrote, "In the past, the hardest security threat to defend against has been the insider threat. That will continue, with untold losses in economic espionage and other security losses."

Mike Liebhold, senior researcher and distinguished fellow at the Institute for the Future, wrote, "Growing pervasive threats will inevitably have an enormously negative impact on: Privacy, e-commerce, finance, infrastructure, and world peace."

Olivier Crepin-Leblond, managing director of Global Information Highway in London, UK, replied, "The probability of a major cyber attack is not 'if' but 'when.' Unless a global cyber-warfare non-aggression pact (like the nuclear non-proliferation treaty, or the treaty against chemical warfare) is signed between the world's powers, chances are that the cyber attacks will be state sponsored. There is also a high chance that cyber attack technologies will be making it into terrorist hands. Without a global cyber-warfare non-aggression pact, it will be impossible to distinguish whether a cyber attack is state sponsored or independent terrorism. To-date there is talk in many locations, including in the Council of Europe, to draft a global cyber warfare convention, but no country around the world is ready to take the first step to engage in such a convention, for fear of giving up its privilege of using such methods in the future. It might indeed be too early to sign such a pact if we cannot know to what extent cyber attacks could cripple our economies."

Ian O'Byrne, a professor at the University of New Haven, wrote, "Governments are beginning to use cyber attacks as a means to wage war. A growing online criminal contingent is beginning to get quite sophisticated with attacks to the general public (e.g., the Cryptolocker virus). These trends will continue. Be sure to do your back-ups, people."

Peter S. Vogel, Internet law expert at Gardere Wynne Sewell, LLP, wrote, "All indications are that cyber attacks will escalate. In particular the recent report from the National Intelligence Council predicts significant widespread harm. Assuming the widespread media reports in 2013 about government cyber directed attacks against other governments and businesses are true, there is no reason to believe this will subside by 2025."

Ian Peter, pioneer Internet activist and Internet rights advocate, wrote, "Tens of billions of dollars is not that much in terms of what damage can be done in a cyber attack, so yes. Equally, I believe investment in countering cyber attacks will exceed tens of billions of dollars per annum if it hasn't done so already. Whether cyber attacks carried out by nations or cyber attacks carried out by individuals pose a greater threat at that time is difficult to guess. Both are likely to become more serious issues."

Jan Schaffer, executive director of J-Lab, developing innovative digital journalism, wrote, "Edward Snowden was smart, but there is surely someone out there who is smarter. Cyber attacks will be (if they aren't already) the Achilles heel of any nation targeted by an enemy."

Dennis McCann, A computer-training director who was previously a senior technical consultant at Cisco and IBM, commented, "As the third and fourth worlds go digital, cyber wars will occur by or to first-world nations. There is no limit to the vulnerabilities of a digital world and this is even today the most significant technical challenge we face."

Charlie Firestone, executive director of the Aspen Institute Communications and Society Program, responded, "There will continue to be an arms race between those seeking to gain access to protected sites, for whatever reason, and those devising protective solutions. Some attacker, at some point in the next 12 years, will beat a country or major economic enterprise that has let its guard down (in terms of keeping up with the latest security techniques)."

Leah Lievrouw, a professor of information studies at the University of California-Los Angeles, noted, "The escalating use of cyber warfare and 'cracking' techniques by 'legitimate' governments, military and law enforcement, and corporate interests, as well as by insurgent political groups, criminal enterprises, repressive regimes, industrial espionage, etc.—coupled with state-sponsored efforts to weaken infrastructure security (e.g., cryptography) to ensure their unrestricted access to data 'anytime, anywhere'—would seem to promise a high probability of a major disruption at some point in the next decade with the potential for extensive harm. Extensive interconnectedness has enormous, demonstrable benefits, and corresponding potential for 'networked' damage."

A research scientist working at a major search engine company responded, "It's constant escalation between them and us (however you define those pronouns). Eventually, a nation-state will launch a serious attack (or maybe just let one get away from them by accident) that will cause a massive information network collapse (e.g., by bricking all the routers on a national backbone network). When that happens, the economic fallout (from uncompleted transactions, inability to deliver time-sensitive information, etc.) will be in the tens of billions. Physical damage will be harder to cause, but still possible. Taking over traffic signals would be one way to do that. Overriding train switching systems or simply jamming all aviation frequencies for a period of a few hours would do the same thing."

Tony Siesfeld, director of the Monitor Institute wrote, "It is only a matter of time. As our lives are stored on our own devices and critical information stored through the system (from doctors to tax authorities to our favorite retailers), we become extremely vulnerable to either an intervention that snoops and steals our information or an intervention that disrupts or disables the network and exchange of information over a wide area for an extended period of time."

Susan Caney-Peterson, a self-employed writer and editor, wrote, "The technically inept and ignorant politicians of the early 21st century in the United States will have acted slowly and poorly to threats from Eastern Europe and China. Attacks will have taken place on the US electrical grid, with Chinese hackers having compromised it back in the 2000s with no one acting on it then. Attacks on individual data will have become routine and only the wealthy will have precautions in place, thanks to the hiring of privacy experts, which become as necessary as tax accountants were in the past. More money will be spent by the government on gathering data on individuals than on national cyber security, until the cyber equivalent of 9/11 takes place."

Peng Hwa Ang, director of the Singapore Internet Research Center at Nanyang Technological University and longtime participant in global Internet governance discussions, wrote, "Because of the greater reliance on networks, should there be an attack on the network, lives will be affected. Already, the cut (deliberate or otherwise) of mobile services has caused deaths in some of the locales of such cuts. It is difficult to imagine no major cyber attack in 20 years."

Francois-Dominique Armingaud, a retired computer engineer from IBM now teaching security at universities, wrote, "Unfortunately, wherever there is use there will be misuses. We can work to limit it, but as with a garden the job must constantly be done. Computers were initially designed without thinking they would communicate. Communications were designed without thinking there would be rogue users. A complete redesign of computer and communication architectures could possibly lead to better security by 2025."

David P. Collier-Brown, a system programmer and author, wrote, "Attacks on old infrastructure, notably power, traffic-lights, railway crossings and railroad switching. Predominantly by non-geographically-concentrated terrorists, as terrorists based in a particular country or state-sponsored attacks invite convention-arms responses. Some on first-generation automated systems like 2013 cars, under the same geographical-origin constraints."

Alex Halavais, an associate professor of social and behavioral sciences at Arizona State University, said, "It may be that we don't even know it is an attack, which is the scary part. The indignation of Google and the rest with the NSA owning their foreign data stores belies the more troubling bit, which is that some of the largest platforms we use are desperately insecure."

Dominic Pinto, a trust and foundation manager active in the Internet Society and IEEE, said, "Forcing everything pretty well online exposes everything to the risk of being hacked—if not by commercial interests and of course the more ordinary criminals but of course as we now know on a huge scale by the state through their security agencies (whether or not the politicians or the bureaucracies actually know and control these activities)."

Rajnesh Singh, regional director in the Asia-Pacific region for the Internet Society, wrote, "I do think we are seeing—sometimes in small doses and sometimes larger—instances of the waters being tested—be it by individuals, groups or entities and nation-states. When nation-states start building cyber defense and attack regimes, there is far much more to it than hype. However, we should be mindful that we don't end up destroying that which sustains us. The Internet, and all that it enables, is a large part of the world economy and has allowed tremendous opportunities for progress and socio-economic development. Any disruption could have a multiplier effect and end up causing unintended consequences long term that may impact the instigator as well. I expect the technical community will rise to the challenge and offer solutions that will continually improve the capabilities of users at large—threats will evolve and so will solutions to the threats."

Miguel Alcaine, International Telecommunication Union area representative for Central America, responded, "Nations, companies, organizations worth an attack, have already started their continuing work to prepare for a potential attack. The race between potential attackers and the ones defending different assets will never stop, and such a race by itself will have a price tag in the billions of dollars if not more. The trend to have some sort of national or institutional defense will continue. It is also healthy to highlight that the lower the defenses of an entity, also the lower the potential profit of attacking them."

William Schrader, co-founder and CEO of PSINet Inc., the first commercial ISP, predicted, "Absolutely, cyber attacks will have massive destructive impact some time in the next 11 years

somewhere on earth. All nations have economic systems which are tightly interwoven among industrial production and distribution, commercial operations, communications, stock markets, financial institutions, personal lives, military and policy operations, and political balance (or imbalance). The critical infrastructure vulnerabilities are known to management of that infrastructure, to the authorities and to those determined to disrupt them. There has been a constant battle among forces to disrupt and forces to maintain during the past two decades. The risk and impact of this type of threat cannot be over-hyped. I choose not to identify specific vulnerabilities or attack scenarios."

David Bernstein, president at The Bernstein Agency, a marketing and research consultancy, wrote, "For every lock, there is someone out there trying to pick it or break in. This is human nature, and I have no doubt it will continue to happen. Yet, I believe that as the threats increase, companies and countries will continue to build more protection, redundancies, and methods to safeguard against criminals. In the past, it has been those inside organizations who pose the greatest risk to security. As a result, I expect greater scrutiny and oversight to those inside our most sensitive areas of national banking, military, and infrastructure."

Thorlaug Agustsdottir, public relations manager for the Icelandic Pirate Party, wrote, "See Vanity Fair magazine's *Enter the Cyber Dragon* from 2011 and the follow-up story from … 2013. This is a huge issue for the years to come. The technical/code aspect of Web crime will become ever more advanced, as will social engineering and phishing methods. Internet security and privacy issues are without a doubt the largest issues of the years to come."

Kalev Leetaru, Yahoo fellow in residence at Georgetown University, responded, "This scenario is quite possible as infrastructure becomes more Internet-connected and the value to hackers increases, and with many rogue states now creating their own cyber armies."

Karen Riggs, a professor of media arts at Ohio University, replied, "Technological advances and implementation reflect values of producers and consumers. As a society increases its dependency on information and communication technologies to assemble, hold, manipulate and share information, it increases vulnerability to its population. This risk includes deepening communication channels among perpetrators whose goals are to create joint action with those whose interests are similar to theirs. Among the most terrible of risks will be using data and manipulating technical communication to collapse economic systems in such sectors as banking and stock markets. Another likely scenario is that enemies of states will infiltrate ICT systems not simply to steal secrets but to push their own agendas, often in subtle ways, through the destruction of data and message integrity. Nations will be less able to maintain filters between their states and citizens. Finally, social and international definitions of threat and enemies of state will continue to

be challenged, as actions by such individuals and collectives as Wikileaks, Edward Snowden, and Anonymous develop greater muscle."

Marc Prensky, futurist, consultant, and speaker, replied, "We are already under massive cyber attacks around the world related to intellectual property. Billions or even trillions of dollars have already been stolen. I believe the concept of intellectual property as we know it won't survive. Little people are unlikely to be harmed in great numbers by this, but countries and their relationships will face major upheavals."

Pamela Wright, the chief innovation officer for the US National Archives, responded, "It is certainly conceivable that there will be a major cyber attack by 2025. In many ways, we are still in the Wild West days of the Internet, with patchy regulations, and huge variances in modernization for basic infrastructure such as power, water and transportation. Private companies spend a great deal of attention ensuring that they can thwart determined opponents. In this age of shrinking government and across the board government budget cuts, I am already concerned about the vulnerability of the public infrastructure."

Bob Ubell, the vice dean for online learning at New York University, replied, "Relentless increases in cyber attacks for consumer information, intellectual property, and government secrets, among other data, is unlikely to abate. Chances are that the spiral will continue to increase exponentially as happened over the last decade."

Gina Neff, an associate professor at the University of Washington, wrote, "More systems will be online created by more vendors. These connected entry points into the 'Internet of things' will create more vulnerabilities for cyber attacks."

Thomas Lenzo, a technology consultant, responded, "So far, major cyber attacks have been made on defense contractors, major financial institutions, and other large targets. Those targets have responded and hardened themselves against future attacks. However, the majority of businesses are small- to medium-size, and they, as well as most home technology users, do not have the defenses needed to thwart a major attack. We will see cyber attacks that cause many of those businesses to go out of business. Recently, a small town lost eight years of its records to a malware attack. The cost of the damage has not been calculated. In the future, there will be more of these types of cyber attacks. As for loss of life, we will see that when a major health care system or a SCADA [Supervisory Control And Data Acquisition] system is the victim of a cyber attack."

Mary Joyce, an Internet researcher and digital activism consultant, replied, "There is no reason to believe that hackers won't continue to out-innovate infrastructure defenders. So long as data

infrastructure is constrained in its function and design and hackers are unconstrained in the methods they can use to infiltrate it, those who own and defend infrastructure will be at a disadvantage."

Danny Gillane, an information science professional, wrote, "The longer the Internet exists, the more people will be exposed to it and to the technology needed to use it for good and for bad. Sooner or later someone—either for political reasons (terrorism, for example) or for criminal reasons—will take down part of the utilities infrastructure leading to economic loss or property loss on a large scale or will steal something or will take down a major economic player, such as Amazon, the Federal Reserve, the Internal Revenue Service."

John G. McNutt, a professor at the University of Delaware, replied, "War in 2025 will be low-intensity conflict and major conflict via technology."

Adam Nelson, founder of Kili.io, a cloud infrastructure in Africa, responded, "The question is whether a major cyber attack will have caused widespread harm to a nation's security and capacity to defend itself and its people. With 200 countries in the world and the fact that so much critical infrastructure is rooted in cyberspace and given the 11-year horizon—it seems inevitable that such an event will happen."

Amy Crook, an IT employee at a large firm, wrote, "Theft in the tens of billions of dollars is definitely possible. Smaller nations have a greater risk of being harmed, since larger nations have more resources to put toward defending themselves from cyber attacks. It will become more apparent that nations such as China are actively working toward goals of cyber attacks on other countries. I don't know how it will threaten a nation's sovereignty. It seems unlikely that allies of any one country will stand idly by if that country is attacked in such a way. I don't know if I can imagine a scenario in which a country is robbed totally anonymously, in part because it would be in the best interest of all other nations to put resources into solving that puzzle in order to protect themselves."

Glen Farrelly, a self-employed digital media researcher and consultant, wrote, "As long as the benefits for cyber attacks remain as attractive as they are now, cyber attacks will continue, which will become only increasingly destructive as more of our lives and societies rely on digital networks."

Bud Levin, a futurist and professor of psychology at Blue Ridge Community College in Virginia, wrote, "I cannot imagine a formal, structured, or government-led defense that will prevent determined, networked, and labile hackers. Offense, by whatever label, can be wrong most of the

time yet still succeed. Defense only has to slip up once, and it will sooner or later. We have thought the virtue of the Net to be its ubiquity and de-centralization. However, we've centralized it in terms of standards and practices and methodologies and overseers, creating new vulnerabilities as we attempt to improve on old. The more standardized and centralized, the more vulnerable to assaultive change."

Scott McLeod, director of innovation for the Prairie Lakes Area Education Agency in Iowa, responded, "We're fooling ourselves if we think that there won't be several major cyber war and/or hacking incidents aimed at governments, not just corporations and other organizations. This is a constant battle right now. It's only a matter of time before something really significant occurs, particularly as more of our physical infrastructure becomes connected to the Web via the Internet of Things and other similar movements."

Daren C. Brabham, assistant professor at the Annenberg School for Communication and Journalism at the University of Southern California, wrote, "There will definitely have been a major cyber attack by 2025. It will probably be perpetrated by the US or China on another country. I believe attacks on a country's stock market or on a country's missile defense system is the most likely application of a cyber attack initially. We will see the development of new major divisions (if not a new branch entirely) of the military focused on military applications of cyber warfare, along with medals and officer ranks for these specialists."

David Solomonoff, president of the New York Chapter of the Internet Society, said, "Likely attacks are getting easier and there a lot of new technologies—medical prostheses, critical infrastructure, Internet of Things, that are not properly secured."

A self-employed interactive communications specialist for a religious news organization responded, "Cyber warfare is no different from other warfare—those looking to harm will find a way and those who are harmed will realize they were not prepared in some way. While advancement will continue and countries will invest more and more in defense, someone will find a way inside—and it could come from within their own country."

A self-employed attorney responded, "Because our businesses and government do not respect privacy, they also do not respect our security. Add to their hubris, the fact that as media companies consolidate and exercise more power, groups like Anonymous will continue to grow and agitate to remind the general complacent public of what is at risk."

An international project manager at Microsoft wrote, "The first major attack on a nation's infrastructure will probably be by terrorists. They could, for example, cause the meltdown of a

nuclear reactor. However, some nations might also start to use cyber attacks that are not easily identifiable as such but cause the loss of lives or major damage."

The editor in chief of an international digital trade journal commented, "We've seen several cyber attacks come relatively close to causing major, widespread harm already. One or more major banking networks are likely to be the first to suffer a catastrophic collapse, and it would not surprise me for full-scale cyber warfare to erupt between China and one or more Western nations. The groundwork for that sort of thing already has been laid."

An anonymous respondent wrote, "There is a clear rivalry between China and the United States and the gap is widening. As the United States is more networked in many areas it is also more vulnerable to cyber attacks. This vulnerability might be used by China and other nations by first striking cyber attacks instead of sending troops."

A webmaster wrote, "Nation-states appear to be engaged in recruiting talent for cyber-war activities. The trend will continue and at some point another war will be fought that will include a cyber front. Likely there will be both direct economic consequences and collateral damage as the utility of cyber warfare is tested."

David Hughes, a retired US Army Colonel, wrote, "It is simply going to happen. First of all in a singular incident, which will then trigger the design and building of parallel or backup capabilities, requiring billions in investment, both government, corporate/institutional, and eventually individuals at their homes."

'Yes' respondents theme 2) Security is generally not the first concern in the design of Internet applications. It seems as if the world will only wake up to these vulnerabilities after catastrophe occurs.

Dave Rusin, a digital serial entrepreneur and former digital global corporate executive, responded, "Cyber attacks are new form of war—economically driven. It is the new reality. Today, America's cyber security is like Swiss cheese. Solutions should be driven by the free market sector as the creativity will be fast and furious. On any given day, most politicians—outside of some briefing of what they want to hear—are not making me feel 'Happy, happy happy …' Our politicians can't listen to generals or intelligence agencies on how to efficiently deal with traditional events leading to war, cyber-what? Eventually billions will be spent by government on cyber whatever—just *follow the money*, we are at risk, because those contracts will have more to do with campaign contributions, who you know, and keeping a politician in office, than an aggressive proactive and defensive-objective, clean, cyber strategy."

Frank Pasquale, a law professor, wrote, “As the wealthy segregate themselves into enclaves or diversify their residences across continents, they (and the political class they heavily influence) will continue to disinvest in infrastructure. Moreover, intelligence agencies and leaders of critical infrastructure will disdain the types of immutable audit logs that could help record and detect and solve vulnerabilities, because they don’t want to be held personally accountable for failures. The situation leaves both electrical grids and banking infrastructures vulnerable to catastrophic attack.”

Brian Butler, a professor at the University of Maryland, wrote, “Since we have not had these (at least not publicly) the will isn't there to deal with it at the level of resources needed. Hence, it is just a matter of time until a perfect storm of unaccounted for vulnerabilities and overconfidence, and external threat coincide. This is another place where the entrepreneurial mantra of ‘fail often’ plus overconfidence will eventually lead to problems, though there is a possibility that the increasing risk aversion among baby boomers, with their substantial influence, might balance this out.”

David Allen, an academic and advocate engaged with the development of global Internet governance, responded, “It depends upon further progress toward global governance schemes—overall—that actually work. By no means is that certain.”

A CEO for a company that builds intelligent machines observed, “We haven't yet had our chance to see the impact of mutually assured destruction on the cyber battle field yet, but the seeds are germinating between the United States and China on this front today, and by 2025 we'll have had our Hiroshima. The problem is that there are several actors here and not all of them are sovereign nations. Any list would include multinationals—who might find an incentive to destabilize a resource-rich government, terrorist organizations—who find fear an ample reason to pull together significant resources), and techno-anarchist groups—who might bring down a power grid or financial market for fun or spite. The threat is very real, and because a profit motive is necessary for anything significant to be done here, I think progress will always be slow. It's easier to get us excited about blowing things up than building yet another defensive wall.”

Dale Richart, a marketing and advertising client liaison, responded, “This probably will not happen by 2025, but perhaps not long after. I do believe I will live to see a devastating event brought about by a cyber attack that will result in a global resolution to abolish some acts of major cyber attack. I doubt we are generally aware of the current level of threat and we need to be exposed to better informative journalism.”

A behavioral researcher specializing in design in voting and elections commented, "The world is a dangerous place. The Internet was built to be free, open, and democratic. That kind of architecture has holes in it, as the NSA has learned (and created with and without the help of corporations that are on the backbone). From my work in voting and elections, I can tell you that one of the major vulnerabilities is in voting systems. Some countries already have Internet voting. Several are piloting elections held online. There is great pressure in the United States to move elections online and states will try it. The advantage that the United States has in the way its electoral system is set up is that it is widely distributed. Conducting attacks during a major election would be extremely difficult considering that there are thousands of voting jurisdictions in the United States that run their own elections. It would be difficult but not impossible. We've already seen election department servers attacked. There's no personal data there that isn't publicly available elsewhere, so that's not the driver. These attacks are practice sessions. They'll probably escalate and expand."

Maureen Schriner, a university professor, responded, "The vulnerabilities to these attacks lies in the nature of the infrastructure, the lack of common governance over the Internet, and the lack of willingness by multinational corporations to change processes. Until a major cyber attack occurs, the people and institutions that control cyber infrastructure won't have incentives to change."

Will Stuivenga, an information science professional in the state of Washington, said, "It is almost inevitable that something of this nature will eventually occur. Human nature and history have shown that effective counter measures will not be implemented until an actual event demonstrates the necessity of doing so. And even then, some nations probably won't have the wherewithal to take effective counter measures, even if they wished to do so."

A professor and CEO with 25 years of experience in technology research and entrepreneurship responded, "There will be many attacks and accidents, many of these with terrible consequences. Whether any single one of them will be to this scale is hard to predict, but we will be able to build and deploy more flexible, more immune-system-type defenses before that happens. It is still too easy for too many deciders to ignore security out of sheer ignorance or because the costs can be externalized. Maybe we need a couple more mega-events before that becomes less of a problem."

Daniel Miller, a professor at University College in London, wrote, "It would be foolish to underestimate the capacity of the military to employ new technologies. And since these work at a distance they will be very attractive. There are obvious imbalances in different nations' capacities to launch and defend themselves from such attacks, which is why it is likely to be successful. Only after which will we see the required international mobilization to prevent further escalation."

A self-employed digital communications consultant commented, “This is just a matter of time. Our government's digital infrastructure is a joke. When giant corporations like Target or social networks like Facebook are having a hard time fending off cyber attacks, it gives you little hope that our government is in any way prepared to handle a big breach. Some country is going to get hit hard. It might not be the United States, but someone is going to have to handle this by 2025.”

Carol Wolinsky, a self-employed marketing research consultant, wrote, “Chinese incursions into the databases of major newspapers, the recent attack on Target and other examples demonstrate the determination and capability of those who wish to disrupt the security and safety of the world's citizens. Al Qaeda and other terrorist groups have similar motivations. The United States lacks the political will to focus on and pay for technology improvements that would slow down or eliminate these threats; the primacy of the United States on the world stage will be in the past and will never recover. Eastern Europe and Asia, where many of the security threats originate, will be ascending.”

Gary Kreps, professor of communication and director of the Center for Health and Risk Communication at George Mason University, wrote, “Serious breaches in cyber-security in the future are inevitable. However, I am hopeful that these serious incidents will raise public concern for security and lead to new programs and policies for safeguarding information systems in the future.”

A law school professor commented, “The grid controls even today. Banking, food, and power are all subject to attack. Those that want to control have always led the way, leaving those that want to help lagging. The question will be the severity of the attack and how widespread. Small attacks happen daily, but don't affect the daily lives of most of the world. Kill the electrical grid in just one major economy and the ripple effect will probably not stop until there is a return to a pre-tech age. A small group can act to bring down a much larger group because of inertia and the human nature of refusing it can happen until it's too late.”

The grants coordinator at academic center for digital inclusion responded, "People are unable to effectively collaborate across systems. Given ample mismanagement and miscommunication already evident, a major cyber attack seems unavoidable.”

Linda Young, a freelance writer, responded, “This nation has done nothing to make sure that the Internet is secure. It has done nothing to ensure that hackers can’t shut down the nation’s water, wastewater, and electrical supply systems. It has done nothing to make sure that banking is secure from attacks. It has done nothing to make sure that medical records can't be hacked and altered.”

A software engineer who works for a major US technology company said, "I fear that computer security by 2025 will not be much better than it is today. We will have more experience, but I expect that the level of complexity of software systems will increase to match. Nonetheless, I don't believe that a major cyber attack will occur. I hope that the fear of an attack will cause critical systems to be hardened/isolated to the point where, although possible, cyber attacks against them will lose their anonymity benefits. At which point, they enter the standard military portfolio and, likewise, will be reserved for times of war. Minor attacks, on the other hand, I expect will continue to be frequent, although will often be carried out by lesser entities than states."

A middle manager in the digital division of a public media company wrote, "We will be shocked by our vulnerability when the inevitable happens. Imagine all the robotic cars crashing into one another, or the discovery of billions being siphoned out of bank accounts. It is the primary risk to our digital future—we may find we cannot accept the risk of our digital vulnerability."

Stephen Abram, a self-employed consultant with Lighthouse Consulting Inc., answered "no" on this question, but his answer suggested he was uncertain fixes would be made. "War seems to always be with us. It's not entirely science fiction that digital security is a moving target and the holes are discovered through attacks and not solved through barriers and moats any longer. If by 2025 we have solved this problem I'd be surprised."

Jon Lebkowsky, Web developer at Consumer's Union, responded, "A cyber attack of the magnitude described here is as avoidable as the Y2K bug, but I wouldn't say it's overhyped. The hype will drive prevention."

A University of Missouri assistant professor of library and information science wrote, "Hackers will probably gain access to more major banks, Internet companies, and the federal government. It's the golden prize. Hopefully it will not happen while I'm flying or driving my robotic car, though."

Liam Pomfret, a doctoral student in digital issues at the University of Queensland, Australia, responded, "Given such events as the Sony PlayStation Network hack, and known vulnerabilities in the US power grid, there's certainly a great deal of potential for an attack causing significant economic harm (though any loss of life would likely be caused only indirectly). Particularly given the Sony case, it's obvious that many large organizations are lacking sufficiently sophisticated security. I don't see many firms taking much more care in this area either, simply because of the cost to them to do so, and the relative lack of punishment they've received from either consumers or governments when such privacy breaches have occurred. Even should a firm be punished, rarely

have the executives who allowed such a situation to occur suffered from any personal liability, making the punishments relatively toothless."

'Yes respondents theme 3) Major cyber attacks have already happened, for instance the Stuxnet worm and attacks in nations where mass opposition to a regime has taken to the streets. Similar or worse attacks are a given.

The IEEE Spectrum publication wrote in February 2013: "[The Stuxnet] worm was an unprecedentedly masterful and malicious piece of code that attacked in three phases. First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself. Then it sought out Siemens Step7 software, which is also Windows-based and used to program industrial control systems that operate equipment, such as centrifuges. Finally, it compromised the programmable logic controllers. The worm's authors could thus spy on the industrial systems and even cause the fast-spinning centrifuges to tear themselves apart, unbeknownst to the human operators at the plant." This reportedly helped slow down Iran's nuclear-material development program by destroying up to a fifth of its centrifuges, though Iran has not acknowledged the problem—and it has been widely speculated that the US and Israel were the developers of the 500-kilobyte worm.

A notable number of respondents cited Stuxnet and other acts against various populations as evidence that cyber attacks were now integrated into national military and intelligence strategies.

David Golumbia, an assistant professor at Virginia Commonwealth University, said, "They already have, repeatedly, and this trend will only accelerate."

Nathan Rodriguez, a PhD student at the University of Kansas, wrote, "It is difficult to envision a scenario where a nation does not experience widespread harm as the result of a cyber attack during the next decade. Iran's nuclear program was dealt a tremendous blow as a result of the Stuxnet virus. I do not think it would be inaccurate to claim the United States is in some ways already amidst a new Cold War with China in the digital realm that will continue to deepen—all under the cloak of plausible deniability."

Jerome McDonough, an associate professor at the University of Illinois, responded, "Given the damage done by Stuxnet and the significant use of cyber attacks in the Georgia/Russia conflict, I suspect we may already have passed the 'widespread harm' [test] you've established."

Andrew Bridges, a partner and Internet law litigator and policy analyst at Fenwick & West LLP, wrote, "Arguably this has already happened with the Stuxnet. An attack on GPS satellite systems

or time stamping systems could be devastating. I don't think the threats relating to these systems have been hyped. I do not know whether major economic enterprises can thwart these attacks."

Adam Rust, a research director for a US-based organization advocating for economic justice and opportunity, wrote, "It is already happening. Cyber attacks are a front in war. Look at what happened in Estonia, in Syria, in Georgia."

The principal engineer for an Internet of Things development company wrote, "Cyber attacks will become an increasingly important part of state against state warfare, as well as becoming a weapon used by non-state 'terrorists.' It has already started with the United States and Israel cyber attacking Iran to cripple their economy and nuclear industry. The next step will probably be more aggressive and open cyber attacks between the West and China."

Lucas Gonze, a respondent who did not share other self-identifying details, said, "Information technology has already been weaponized. Nations are already in hot conflict. Cyber attacks have been waged. With the Stuxnet/Flame attacks on [the Iranian nuclear plant] Nataanz, the Iranian capacity to build nuclear weapons was reduced. It is entirely possible that tens of billions have already been spent by the Iranians. So this question is not very theoretical. If the question is whether major powers such as the United States or China will suffer such losses, that is an ideological slant in the question."

An assistant professor at New Mexico State University wrote, "The cyber Cold War has already had some hot skirmishes in the 2000s. It seems likely that there will be some significant casualties by 2025. The US-Israeli developed suite of cyber-weapons known as Stuxnet has already demonstrated a more complex suite of behaviors than many experts had imagined when deployed against Iran (and probably other targets as yet undisclosed). Unlike nuclear weapons, which require heavy industry and large investments of time and resources to develop and deploy, cyber-weapons are extremely cheap and require little more than brains, information, and readily available inexpensive hardware to develop and deploy. In this game, the attacker has an enormous advantage, because very few of the millions of possible target systems were designed with defense against cyber-attack in mind."

'Yes' respondents theme 4) Cyber attacks are a looming challenge for businesses and individuals. Certain sectors, such as finance and power systems, are the most vulnerable. There are noteworthy divides between the prepared and the unprepared.

Steve Jones, a distinguished professor of communications at the University of Illinois-Chicago, responded, "I don't think this is likely, though it isn't impossible. One of the things that causes

some hope is that most critical systems are not interconnected (Internet notwithstanding) so an attack on one is unlikely to disrupt others. The one that may be most vulnerable, as we've seen in the recent simulated attack, is the electrical grid, and there is certainly potential for attack and serious disruption via that vector."

Bryan Alexander, senior fellow at the National Institute for Technology in Liberal Education, responded "no" but elaborated, "The real research and development in this field isn't directed at nations. Instead it's about taking money from those who have it—i.e., crime. National cyber attacks seem to be tending less towards the notorious 'electronic Pearl Harbor' and more towards harassment and sabotage. So we can expect successors to Stuxnet: 'Oops, it looks like a Chinese aircraft carrier lost power for a day.' 'Huh, the American embassy in Paris is suffering a DDoS attack.'"

Neil McIntosh, a British journalist working for a major US news organization, wrote, "It would be easy enough to worry only of Hollywood-style attacks on infrastructure; electricity grids, military facilities, and so on. I'm sure there's risk enough there. But greater, more realistic (and harder to defend against) danger may lurk in less glamorous places. For instance, the global banking industry has individual players whose failure would, on their own, bring their host nation to its (financial) knees. This would undoubtedly have an impact on that nation's sovereignty and—by extension—its ability to defend itself. It doesn't take a huge leap to imagine a situation in which a major financial institution finds its systems under attack; an attack that, then, brings into play those huge sovereign risks. I'm afraid I find this scenario plausible."

Andrew Chen, an associate professor of computer science at Minnesota State University-Moorhead, responded, "The 'smart grid' is the most substantial danger. Cyber attacks that target a 'smart grid' will result in loss of power to large numbers of places simultaneously, causing infrastructure damages. Likely places that this will cause substantial damages will be airports, trains and train stations, draw bridges, traffic signals, and so on. No single instance will be 'widespread harm,' but all of these together will add up to that in only a short period of time. Unless there is some unforeseen major new technological development (such as widespread availability of quantum cryptography-based one-time-pads), the only way to prevent this will be to refrain from adopting 'smart grid' technologies."

Meg Houston Maker, writer, editorial strategist, and private consultant, responded, "I'd like to believe that cyber attacks would be more likely to cause property and national security breaches than loss of life, and that they're more likely to occur in less developed nations, or regions experiencing conflict or warfare. However, it seems clear that messing with the national grid

during times of extreme weather events or hacking the public transportation system could pose a vital threat."

Matthew Henry, a CIO in higher education, replied, "Cyber attacks will be huge and will cause physical and human life loss. Vulnerabilities within utilities will be the greatest danger, followed by dangers to medical areas. Financial vulnerabilities will continue to the level of causing loss of assets to corporations, governments, and individuals."

Larry Magid, technology journalist and Internet safety advocate, wrote, "It is my hope and belief that those responsible for physical infrastructure will find ways to isolate critically important systems from a vulnerable grid. I do think that banking and information services will remain vulnerable but not things like power plants and water systems. My big worry though is whether autonomous vehicles and drones might be increasingly vulnerable."

Jesse Stay, founder of Stay N' Alive Productions, replied, "It won't be what you think, though. Citizens will have more control over their own security rather than the nation controlling cyber security. As such, the citizens who are more security conscious will be more protected than those that are not. Currencies such as Bitcoin will also be more prevalent, and the need for citizens to know more about their own security will become even more important. Citizens will get smarter, and will be more empowered to protect themselves."

Brittany Smith, a respondent who did not share a professional background, wrote, "Cyber attacks and cyber security will be the issues that define the upcoming decades. What is unfortunate is that many Americans are unfamiliar with cyber security and do not know how to protect their own information. Education and collaboration across sectors will be necessary to help us protect ourselves individually and collectively."

Kevin Ryan, a corporate communications and marketing professional, responded, "Military and business will probably have their own special Internet with a great deal of protection. Enough cyber attacks have been occurring that the military will make security a priority. Well-funded corporate entities will follow suite with special networks. The common man will be vulnerable."

An administrator for technology-focused units in educational nonprofits responded, "Vulnerabilities ripe for targeting by hackers may be found in the following areas, both public and private: power grids, financial institutions, defense institutions, medical institutions, educational institutions, business enterprises, and any other institutional gathering place or space. Most people and the institutions they inhabit or maintain are not yet attuned to being vigilant about

keeping technology-enhanced spaces secure; thus, they are more careless and inattentive than they should be, especially in the face of known, not hyped, hacker persistence in invading such spaces."

Evan Michelson, a researcher exploring the societal and policy implications of emerging technologies replied, "Attack is likely yes, but in addition to targeting national security and corporate targets, such cyber attacks could be aimed at small businesses. Imagine a denial of service attack planned for 'Small Business Saturday' that targets local payment systems. The level of threat is higher than we currently expect."

Some responses that straddle 'yes' and 'no'

Several respondents in their narrative answers discussed the pros and cons related to likely cyber attacks and had answers that fit between the poles.

Raymond Plzak, former CEO of the American Registry for Internet Numbers, and current member of the Board of Directors of ICANN, wrote, "I would say significant yes, but widespread, no. Just as previous threats over the course of history were thwarted or averted, others succeeded by the use of surprise often coupled with innovation. Such will continue to be the case in the future. Only a thorough understanding of the environment and the ability to anticipate the outlying case or method while not fixating on them will continue to be the path to success."

Lyman Chapin, co-founder and principal of Interisle Consulting Group, wrote, "Responding 'no' is a counter-intuitive answer to this question, but consider that the opportunity and the motivation to carry out such an attack have existed for at least a decade. The question really hinges on what we interpret as major. There will be cyber attacks, and damages will ensue, but I think enough diversity has been built into the system to enable it to survive."

Dave Burstein, editor of Fast Net News, responded, "The US and other countries are spending billions of dollars developing cyber warfare capability and actively using it in modest ways. If we continue to have wars like Iraq, Afghanistan and the cold war against Iran we will likely use our capabilities. Yes/no is not the right way to answer this; it's really 'maybe.'"

Tim Mallory, an information science professional, responded, "The value of the damage is in the eye of the attacker and the victim. What may be seen as 'billions of dollars of value' may be meaningless to most people."

A law school professor commented, "The grid controls even today. Banking, food, and power are all subject to attack. Those that want to control have always led the way, leaving those that want to

help lagging. The question will be the severity of the attack and how widespread. Small attacks happen daily, but don't affect the daily lives of most of the world. Kill the electrical grid in just one major economy and the ripple effect will probably not stop until there is a return to a pre-tech age. A small group can act to bring down a much larger group because of inertia and the human nature of refusing it can happen until it's too late."

An editor focused on how technology affects policy and society for a major US online news organization responded, "I agree with those who say that the cyber security threat is much like the Cold War nuclear threat: there is both an arms race and concern about mutual assured destruction. I believe that there will be many, many small and medium-size cyber attacks between now and 2025, but nothing on a major scale."

An economist for a leading Internet company responded, "I can see attacks that will create inconveniences and monetary loss, but I do not expect widespread harm from pure cyber attacks. New and better forms of secure identification will emerge, which will help with many security issues. New crimes will appear and old ones will disappear, be we will not see dramatic changes in the overall level of criminal and terrorist activity."

Themes among those who responded 'no' there will not be major cyber attacks

'No' respondents theme 1) There is steady progress in security fixes. Despite the Internet's vulnerabilities, a distributed network structure will help thwart the worst attacks. Security standards will be upgraded. The good guys will still be winning the cyber security arms race by 2025.

David Cohn, director of news for Circa, responded, "It is, of course, a constant game of one-upsmanship. Criminals get bigger guns, defense gets bigger guns, and so forth. However—short of a major leap—the checks and balances here minimize the harm."

Kevin Carson, a senior fellow at the Center for a Stateless Society and contributor to the P2P Foundation blog, wrote, "I expect a lot of small-to-medium attacks will lead to extensive decentralization and hardening, and to the degraded functioning of all large, visible institutions."

Giuseppe Pennisi, an employee of the Economic and Social Council of the Republic of Italy, said, "I feel the era of major cyber attacks is over."

Bill St. Arnaud, a self-employed green Internet consultant, wrote, "Businesses, research groups, network operators, and various Internet organizations have taken considerable steps in the past

few years to thwart wide-scale attacks. The demise of the Internet from attacks has been predicted for years. There will still be thousands of small-scale attacks per day, but wide-scale, economically crippling attacks are extremely unlikely."

Laurel Papworth, a social media educator, commented, "This is unlikely as we move to peer-to-peer networks the public are pretty good at spotting and dealing with threats, certainly members of the open source community are, more so than closed systems. It will be less vulnerable, not more."

Even though he answered "yes" on the question, **Nick Wreden**, a professor of social business at University Technology Malaysia, based in Kuala Lumpur, sounded a similar theme: "The Internet was designed as a distributed system. This means that attacks can be localized or even blocked if necessary. One reason Libya shut down its Internet connections to the outside world was fear of attacks on its military infrastructure."

Similarly, "yes" respondent **Clark Sept**, co-founder and principal of Business Place Strategies, Inc., made this point: "Those nations that are vulnerable as targets today are largely mutually vested and invested in avoiding such a catastrophe. Notwithstanding rogue agents, cyber security is today and will continue to be a major area of investment in the coming years. As a matter of global fiscal policy, the major players (nations and their central banks) are continuing to be mutually intertwined financially and, as such, will quietly agree in back-room style to stay clear of such cyber warfare, and to put in place appropriate measures to ensure cyber hegemony cannot occur."

Dean Thrasher, founder of Infovark, Inc., commented, "I find it difficult to believe that modern, critical systems would be built without fail-safes, overrides, or other controls that could be used in the event of an emergency. Cyber attacks will continue to cause disruptions to companies and individuals, and perhaps entire government agencies, but it's hard to imagine a cyber attack that would pose an existential threat for any nation."

Christopher Wilkinson, a retired European Union official, board member for EURid.eu, and Internet Society leader, said, "Governments and corporations will invest heavily in thwarting attacks. There will be more cyber attacks, but damage on the scale suggested above is unlikely."

Stuart Chittenden, the founder of the conversation consultancy Squishtalks, replied, "A tit-for-tat incremental escalation will arise, not a single catastrophic 'hack' or cyber assault. As one entity institutes a capacity to create or exploit a vulnerability, other entities will be developing remedies."

Peter Janca, managed services development lead at MCNC, the nonprofit regional network operator serving North Carolina, commented, "The incremental nature of attack escalation is enabling governments and private entities to keep up, or at least not get so far behind that an earthquake event like the World Trade Center attacks of 9/11 is likely to happen."

John Saguto, an executive decision support analyst for geospatial information systems for large-scale disaster response, responded, "It will not get this extreme. Whatever is 'done' can be 'undone,' so the paranoid 'loss' issue is more of inconvenience than real loss, perhaps there will be varying degrees of 'loss' not noting that will shift the balance of power. Now, nature on the other hand, is another story."

Avery Holton, a professor at the University of Utah, said, "Security against such attacks is keeping pace with the attack planning. While there may be smaller scale disruptions, a major attack should not occur."

David Burstein, CEO at Run for America and author of *Fast Future: How the Millennial Generation is Shaping Our World*, commented, "There will likely have been a collective group of smaller attacks by 2025, which in aggregate will have caused widespread harm, but the attacks we are going to see are more likely to be smaller individually than a so-called doomsday scenario. The most likely scenario will be ongoing corporate espionage, which by 2025 will allow companies in other countries to hack into American corporate systems and steal trade secrets to either rip-off individual products or to advance their own place in the market."

Even though he responded "yes," **Bryan Padgett**, a research systems manager for a major US entertainment company, spoke to this theme in his answer, "With the increased visibility on cyber security, more academia partnerships and companies are building operating systems and other products with security and redundancy in mind from the ground up, instead of trying to apply it after-the-fact on top of what was already created. There will no doubt be more exposure, especially as everyday items start to become connected, but enough protection will come from new areas of cyber security and cybercrime defense."

Beth Bush, the senior vice president for a major healthcare professional association, said, "I believe that the United States has the computing power, the intelligence, and the ability to apply these to avert physical harm in the event of any cyber or other type of attack."

Kit Keller, a researcher and consultant, responded, "While the terrorism threat to the United States is real, I am optimistically counting on cooler heads to prevail in terms of our international

relations. Right now, Americans are hated in many parts of the globe. With a change in our policies this can be altered. If we're not as hated, we're less of a target."

Lisa Dangutis, webmaster for The Sunshine Environment Link, wrote, "People have tried and failed in the past. The biggest threat to any countries security is data mining or logistical attacks. Which has happened in the past and succeeded. However, to date data mining has not cost lives or property loss and logistical attacks are generally caught. Theft of money is a risk with any computer system, but I think for harm we need to include human loss or property loss. Crash of a financial system would be bad, but it would be nearly impossible to harm an entire country. There are too many back ups in place. I don't believe by 2025 it could happen on a national level. However, I believe there could be serious attacks to liberty but not enough to cause large widespread harm like Super-storm Sandy."

An anonymous respondent predicted, "Information technology systems will remain sufficiently protected, and sufficiently fragmented, that widespread harm from attacks are unlikely. Additionally, there are significant economic disincentives to launch of a cyber attack from an organized nation-state—once a given country was identified as the source of an intentional attack, they would effectively be cut them off from large portions the Internet and that would cripple it economically. However, I do expect cyber attack strategies to gain in sophistication and effectiveness. Phishing attacks will continue to be effective as attackers are increasingly successful in disguising their intentions and at crafting deceptive communications. Username and password credentials, already often weak or traded on the black market, will be considered insufficiently secure for most sensitive transactions such as online banking, and will be replaced or augmented as a matter of course with easy-to-use two-factor authentication."

Riel Miller, the head of foresight for UNESCO, based in Paris, wrote, "Assuming that vintages of systems remains significant—meaning that the vulnerability of uniformity is avoided—no one attack can be too devastating. Only if some so-called 'brilliant' plan manages to create a unified and homogenous infrastructure will this kind of danger really become serious."

Michael Glassman, an associate professor at Ohio State University, said, "There may be attempts at cyber attacks but they will not be extraordinarily damaging. There are a couple of reasons why this isn't as big a problem as it could be at this point. First it seems it is much easier to play defense than offense on the Internet. Defenders can move quickly and always understand their program much better than an intruder. Also the best hackers tend to be apolitical and very independent. They would be difficult for a government to recruit and would be much more likely to work as part of a crowd sourced response to a state attack."

'No' respondents theme 2) Deterrence works, the threat of retaliation will keep bad actors in check, and some bad actors are satisfied with making only small dents in the system so they can keep mining a preferred vulnerability and not have it closed off.

Thomas Haigh, an information technology historian and associate professor of information studies at the University of Wisconsin, responded, "As the Internet becomes ever more vital it remains inherently vulnerable and the opportunities for an economically disruptive attack continue to grow. Likewise, as more power, transportation, and other systems are coupled to the network there will be real opportunity for physical disruption. However, I would expect the threat of conventional retaliation to deter such attacks just as, for example, it has prevented state-sponsored chemical weapons attacks."

Fernando Botelho, a social entrepreneur working to enhance the lives of people with disabilities wrote, "International actors with the know-how and resources to mount a meaningful attack will not do so, as they are equally vulnerable. This is not to say that minor highly-visible attacks will not be used in political posturing."

Uta Russmann, a professor of strategic communication management and new media based in Vienna, Austria, wrote, "A few nations will always have the knowledge and institutions (e.g., NSA spying on German leader Merkel) to thwart determined opponents as this is a situation in their focus."

Thad Hall, an associate professor of political science at the University of Utah, wrote, "Such an attack is completely possible—the nation's cyber security is quite porous—but the actors who have the greatest ability to pull off such an attack (another sovereign state) would be hurt because of the collateral damage."

Even though he answered "yes" to this question, **James Penrod**, former CIO at Pepperdine University, the University of Maryland at Baltimore, California State University at Los Angeles, and the University of Memphis, struck this note: "There are enormous dangers to all nations and especially to the most highly developed nations, well beyond what most US citizens can imagine. However, the destructive power of such a war is so great that the leaders of developed nations will find ways to maintain an uneasy peace, as was the case in the Cold War. Should this not occur, the world might experience another dark age!"

Andrew Pritchard, a lawyer and PhD candidate, wrote, "The Cold War idea of mutually assured destruction should limit the prospects for all-out cyber war just as it did for nuclear war. A crippling cyber attack on a scale that jeopardizes national security or economic survival requires,

at least for now, expensive technical capabilities and an impressive concentration of expertise. Most of the actors with the ability to put such resources together are national governments and large corporations—the sorts of rational actors unlikely to expose themselves to a proportional counterstrike."

A law professor at Georgetown University and former Federal Trade Commission official wrote that while the first major attack might not be deterred, that model will likely be implemented in the long run. "A serious cyber attack is almost inevitable, notwithstanding concerted and well-intentioned efforts to guard critical infrastructure to protect against such an attack," he wrote. "My sense is that at some point, this will become a global issue, and cyber-protection agencies around the world will band together to root out non-state attackers. Whether we'll ever be able to safeguard ourselves sufficiently from state attackers is hard to assess, but at some point the same arguments for mutual deterrence—mutual assured destruction—might actually mitigate the risk. It is despairing to talk about this in Cold War terms, but at some point, the capacity of state actors to inflict massive harm on one-another through cyber attacks may become the best deterrent of all."

'No' respondents theme 3) Hype over cyber attacks is an exaggeration of real dangers fostered by the individuals and organizations that will gain the most from creating an atmosphere of fear.

Peter McCann, a senior staff engineer in the telecommunications industry, responded, "The potential for destructive terrorist acts carried out through computer networks has been dramatically over-hyped. To the extent that computers are put in control of life-critical processes, there will be air gaps and safeguards in place that prevent malicious outside instructions from interfering in their operations."

Darel Preble, executive director and founder of the Space Solar Power Institute, wrote, "The major damage to our national power grids is not from cyber attacks but from natural causes—squirrels, ants, ice, falling trees, wind, and simple human error."

Ousmane Musatesa, an academic and self-described citizen of the world, wrote, "All these supposed threats are just scarecrows to push citizens in such a big distress that I give up all decisions to the association politics-economics powers."

An anonymous respondent responded, "This is an overblown idea stoked by totally paranoid cybersecurity people. If terrorists wanted to take out the electrical grid, for example, they could do it a lot easier with bombs as opposed to having to mount a cyber attack. Only when cyber is cheaper and easier than bombs, guns, gas, nukes, and biological will cyber have any real threat.

Right now cyber attacks are too costly. The bigger risk will be when cyber crooks drain Wall Street of all its cash. Now *that* is more likely."

A director at Defense Distributed wrote, "This form of 'cyber war' is a nightmare scenario used by mostly Western governments to justify their own cyber operations, systemic oversight, and 'kill switches.' This scenario is not realistic even in 2025."

Even though he answered "yes," **Aziz Douai**, a professor of new media at the University of Ontario Institute of Technology in Canada, covered this same ground: "While it is probable, I think a major cyber attack will not happen by 2025 because insurgent groups and 'terrorist' organizations will lack the capability to launch such an attack. The hype surrounding the threat of cyber attacks will continue for various reasons including the fact that it justifies the infringement on privacy, setting up a panopticon-like Internet infrastructure, and the allocation of excessive budget for cyber warfare and security."

A lecturer and researcher at a public university in Australia responded, "All of this talk about cyber attacks is meant to frighten us. It may be possible but the possibility is akin to the threat of nuclear attack in the 1950s, designed to keep us worried and allow agencies to protect us. I feel we are already under a form of cyber attack every time we leave the house or go online—by companies we have no idea about and by government agencies. Why might cyber-attacks be expected and from which quarter? Possibly by those who feel they are also entitled to benefit from advances in technology, but have been denied free access to those benefits? I am unable to answer the question posed, as it brings up too many questions of my own, e.g. how to 'successfully thwart'? Perhaps by pre-emptive strike? I do not see these issues in black and white and therefore I cannot answer successfully or without some cynicism."

An engineer at an Internet company responded, "The cyber war threat is mostly described by retired generals turned consultants who are more eager to sell their book than to help improve the security of the Internet. My guess is that the 'natural' Internet resiliency will make it easy to inflict local damages (we have already witnessed that many times) but very hard to inflict widespread damages."

The digital editor for a major global news organization responded, "I am skeptical about the digital Pearl Harbor scenario; those who advance it have obvious vested interests in doing so. I think Thomas Rid's thesis that cyber war will not take place has a lot of merit; this is really just a silly new name for sabotage, espionage, and subversion. The analogy with war is negatively useful."

Above-and-Beyond Responses: Part 2

A range of input by some respondents covered ground not related to the themes highlighted above.

Put this in perspective—many things are worse and could have a more devastating effect, including natural disasters and the impacts of rapid online financial transactions

Ben Shneiderman, professor of computer science at the University of Maryland, wrote, "Cyberattacks will grow, but defense will improve, all requiring big investments and creating jobs. Epidemics, tornados, floods, and earthquakes will still be more deadly. Climate change and environmental destruction are by far the greatest threats."

Jari Arkko, Internet engineer with Ericsson and chair of the Internet Engineering Task Force, answered this question "no," explaining, "It is hard to predict what will happen. A single financial transaction gone wrong or a single-vehicle accident could cause the damage that you ask about. But I still consider the risk of these events far smaller than many other similar issues, certainly far below financial fraud that we've used to seeing from insiders and rogue traders, for instance."

Brenda Michelson, a self-employed business-technology consultant, responded "yes" and sounded a similar note. "In the case of cyber attacks, the hype of pending calamity is probably a positive, as it increases threat awareness and in turn (hopefully) prompts telecommunications, transportation, energy, water supply, and food-chain infrastructure operators and regulators to engage and invest in risk-mitigation activities, as well as theorize, scenario plan, and test for systemic, cascading implications. If a nation were to fall, or be seriously harmed by cyber attack, it would have to be a highly coordinated attack, simultaneously targeting the nation's various infrastructure elements; or an attack that could identify and exploit a linchpin element, resulting in cascading failures. This type of destruction is more likely to be brought on by nature—hurricane, tsunami, earthquake, and such. Which, I suppose could be—or certainly hyped as—a 2025 cyber threat, weather hacking."

A proposal to use decentralized network protocols

Andrew Rens, chief counsel for The Shuttleworth Foundation, wrote, "My answer could equally well be 'yes unless appropriate changes are made' or 'no if appropriate changes are made.' Whether a major cyber attack causes widespread harm depends on whether some systems are changed in order to prevent not attacks but the likelihood that they will be widespread. It is certainly possible to configure networks so that they are both highly connected (with few links between most modes) and modular with weak links between strongly connected clusters. In the events of disaster, such as attacks, the weak links must be broken so that only specific clusters

suffer damage. A cyber attack must be understood from a network architecture perspective as a type of disaster, as are natural disasters and internal system failures. What must be done is in principle obvious, although implementation may prove difficult. 1) End centralization of systems such as control of power grids and instead use decentralized network protocols to manage co-operation. 2) Make networks modular so affected clusters can be isolated. 3) Build in overrides that enable the decoupling of local physical systems from digital systems so humans can operate systems when computers fail. 4) Encourage the creation of robust cities that can generate their own water and power at least in need. 5) Decentralize the financial system so there are not just a few players that are massively dependent on one another but many more players. Reinstate the Glass-Steagal Act so that damage to investment banks doesn't affect the day-to-day activities of people. While what must be done is obvious it is unlikely that policy makers and business leaders will demonstrate the will to protect their citizens. Instead there is likely to be a proliferation of agencies with draconian powers engaging in intrusive, if no longer universal, surveillance which are unable to prevent or mitigate attacks because the solution is decentralization not policing."

The concept of the nation-state is being challenged

David Orban, the CEO of Dotsub, wrote, Yes. "Nation-states are under attack from much bigger forces than cyber hacking or from cyber war initiated by other nations. These can and will be waged, and the infrastructure to defend against them will be an important component to be developed and deployed. However, the more radical transformation of all the major components of what is today the *raison d'etre* of the nation-state is going to have a much more radical impact, transforming the social organization, and the social contract itself, to be based from a centralized hierarchical structure to a distributed, peer-to-peer one. Solar power in energy production, 3D printing in manufacturing, plant labs and meat cultivation for food production, self-directed open learning, personalized health, distributed digital currencies."

Relatedly, **Karen Landis**, the user-experience team lead for Belk.com, a department store, said, "People will get used to identity theft and cyber attacks in the way we got used to muggings and bombings. They won't surprise us and will just be something that is in the news every day. Words like 'identity' and 'nation' will have to be redefined. How are you part of a 'nation' when you are connected globally? If the currency system becomes global (e.g., Bitcoin), nations will not be as necessary."

Threats could be domestic more than foreign

S. Craig Watkins, a professor and author based at the University of Texas-Austin, said, "This is something that could happen, but is something that government agencies and corporations are vigorously addressing in their efforts to protect the nation, people, resources, and institutions

from such injury. Efforts to inflict such harm are already in progress, hopefully the intelligence communities are designing ways to identify and address such efforts. Also, while we have thought about these attacks from foreign agents, it's also prudent to consider that it could be internal or domestic threats."

Defenses can result in vulnerabilities

Estee Beck, a doctoral candidate at Bowling Green State University wrote, "In Nicholas Carr's recent article in The Atlantic [*All Can Be Lost: The Risk of Putting Knowledge in the Hands of Machines*], he discusses the occurrences of software malfunctions in computer software systems in aircraft carriers that resulted in loss of life. Even as the American public has learned more about the NSA's efforts to set up defense systems in cyber systems, some of the very defenses they set up also result in vulnerabilities that can be exploited. While I do not necessarily foresee a widespread dystopian future where an entire cyber network crashes, there are already signs of harm occurring, the Dow Jones flash crash, for example. It is plausible to consider that cyber attacks can result in widespread harm considering past events."

Quantum computing requires new levels of security

Mattia Crespi, president of Qbit Technologies LLC, responded, "The modeling of complex algorithms and new forms of processing power will determine the need of new levels of security. On the edge on quantum computing, the world is about to face the need of a new standard for security. The bridge from a 'now relatively secure world' to a new 'truly secure world in the quantum era' will be full of pitfalls and dangers. Terrorist attacks may find their ways in a system adapting its security standards."

Bigger economic, social, and political issues should get the focus

Marcus Cake, network society content architect and strategist with WisdomNetworks.im, responded, "Major cyber attacks are likely and will cause widespread harm. However, the harm caused by cyber attacks in a network society will be a fraction of the harm caused by hierarchies in the Information Age. Hierarchies in the Information Age cause widespread harm. Harm includes unsustainable income inequality, national insolvency, personal insolvency, war, collapse of global and national financial systems, bank insolvency, high-risk leverage ratios in financial and other institutions, money printing. It is unlikely that distributed structures that provide full transparency, distributed income, productivity, and distributed prosperity with collective wisdom and community participation would lead to many of the harmful events of the Information Age that are possible due to opaque unaccountable hierarchies."

Stealing an election? The most vulnerable systems might be tied to voting

Barbara Simons, a retired IBM computer scientist, former president of the ACM, and current board chair for Verified Voting, responded, "I don't know how you measure the value of democracy in financial terms, but if we move to Internet voting, which is a real danger, we run a very serious risk of having elections stolen. Internet voting is vulnerable to attacks by anyone from anywhere, including insider attacks. And of course it's impossible to conduct a recount to determine whether or not the declared results are correct."

Digital systems are vulnerable, but they can also be used to advance the public good

Nishant Shah, a visiting professor at The Centre for Digital Cultures at Leuphana University in Germany, responded, "This presumes that there is a disjoint between the digital infrastructure and the national sovereignty, whereas we have only seen that there is symbiotic relationship between the two. As the digital evolves, surely, the very idea of what a nation is, where its territories are, and how it governs itself are also changing. And as nations become more digital in their organization and logic, they will make themselves vulnerable to cyber attacks—but they still own and possess a vast infrastructure of the digital and the cybernetic and will be able to shift attentions and resources in producing defenses which are in the interest of the people."

The threats are there—so are the problems caused by overreaction to them

Lillie Coney, a legislative director specializing in technology policy for a member of the US House of Representatives, said, "The Internet is like oxygen. If you do something to it in one place it will likely impact the quality of oxygen in other places. An attack may happen but the impact will likely lead to the same reaction to poison gas or chemical weapons that resulted from World War I. My greater concern is an accident or a new application or technology that adversely impacts the way the Internet functions. The other greater threat is to monetize the Internet by controlling who can have websites, use an email address, or communicate. The early days of radio were open and anyone could broadcast. That soon gave way to a regulatory framework that used the cost of licensing to control who could own a station. Innovation became proprietary and it basically stopped making changes. Radio remained essentially the same."

Marc Brenman, a faculty member at Evergreen State College in Olympia, Washington, wrote, "This is already happening. 'Sovereignty' is already becoming an antiquated concept, as borders become permeable and globalization takes command. Anything attached to the Internet or the cloud is vulnerable to remote control and destruction. Just as individuals will have no privacy, corporations and nations will be penetrated. Theft will replace invention and intellectual property. The Chinese and the National Security Agency are already demonstrating this."

‘We have no idea how bad the situation really is’

Norman Weekes, a volunteer for a nonprofit, responded, Yes. “Crime and attacks will gravitate to and come from parts of the world without investments in cyber defenses: Africa, South America, Eastern Europe etc. The level is under-hyped for the same reason financial institutions don't talk about successful robberies; it's bad for business. We have no idea how bad the situation really is.”

Rise of powerful hacker culture

Anita Salem, a design research consultant, responded, “Long before 2025 we'll see cyber attacks on networked physical infrastructure. Also, weapons systems and information systems are at risk. This is one of the likely disruptors to all of the doom and gloom predictions I've made earlier. A large-scale attack may actually lead to less centralized control and more interdependent networks being developed. I expect as technology deepens the economic divide between nations and within the United States, we'll see the rise of a powerful hacker culture that will expose and take advantage of cyber weaknesses.”

Systems are especially vulnerable

Alison Alexander, a professor at the Grady College at the University of Georgia, wrote, “Quite possibly is my real answer. While I do agree that the level of threat is hyped, the potential is there. Downing the power grid, even messing with traffic control, or wresting control of important systems that are currently automated is frightening and certainly possible. Hackers can do these things. Other threats are just as worrisome: hacking into banks or Social Security databases could result in major monetary losses. Finding digital ways to manipulate world stock markets is all too possible. We can talk about existing vulnerabilities, but the ones that will cost the most are the ones we don't know.”

Vittorio Veltroni, CEO for Hyppo Corporation, a digital and customer-knowledge consultancy, wrote, “As repetitive, rule-based tasks shift towards machinery, so does the running of complex networks (energy, water, transport, financial transactions). Those will become targets for disruption by external and internal threats alike.”

Cyber attacks will be aimed at powerful nations by the less powerful

Leigh Estabrook, dean and professor emerita at the University of Illinois, wrote, “If the United States continues a foreign policy of domination and threats, some of which have been cyber attacks on other countries, what do small countries with little chance to fight militarily do? I don't know if a major cyber attack will occur; but it would seem a good possible response of David to Goliath, even in the modern retelling of that tale.”

A long-time scholar and activist focused on the commons said, “Yes, attacks are imminent, especially if governments do not adapt to the networked culture and recognize that top-down coercion without genuine democratic participation and consent (beyond elections) is essential to trust, legitimacy and efficacy in governance. There will always be ‘evil geniuses’ seeking to wage cyber attacks, but some cyber attacks amount to proxies for democratic discontent that political and economic elites, in defending the powerful institutions that they direct, wish to ignore or override.”

The spread of cell phones is the real vulnerability

A retired information science professional observed, “A Rutgers’s University study disclosed that malicious software for cell phones could pose a greater risk for consumer's personal and financial well-being than computer viruses. People are multitasking with their phones for work, personal life, and finances. The risk of malware is high and the sheer number of phones being used for banking and transfer of work information points to losses that can easily reach the levels of billions of dollars. Banks and other financial institutions are vulnerable to attack especially in regard to debit and credit cards. People felt that PIN numbers gave them an additional layer of security for their accounts but the recent problems at Target stores emphasizes their vulnerability. The Edward Snowden case shows that a cyber attack isn’t the only way to get information that could damage a nation’s sovereignty. Many of our current cyber attacks from outside sources are aimed at our military security but agricultural information can be just as important. Information regarding research and development can have a huge impact in many areas of our economy. Maintaining vigilance will help thwart these attacks. Reading the history of the Stuxnet virus is an interesting view of how malware targeted an industrial system.”

A high-altitude electromagnetic pulse attack could be devastating

The CEO of a software technology company and active participant in Internet standards development, responded, “This is likely to happen and could be either a literal cyber attack or a high-altitude electromagnetic pulse (EMP) attack; the latter would cause longer lasting damage. We are increasingly dependent on complex software systems and the migration to more dynamic virtualized infrastructure makes these even more complex. Governments, banks, and other large infrastructure providers will use highly virtualized systems well before 2025. There have been major outages with cloud-based systems even without a cyber attack—a well organized cyber-incursion could potentially wipe out storage systems that contain application images and data, making recovery long and complex.”

The US is reaping the whirlwind of its surveillance programs

An Internet engineer and machine intelligence researcher wrote, “Cyber attacks will continue. Some will be more effective than others and some will be more publicized than others. The loss of personal privacy has already caused widespread harm to the United States and some other nations. If to defend a nation's people includes defending the principles that define the nation and the individual rights and freedoms afforded to the people by those principles, then the NSA has mounted the most damaging cyber attack to date, with no apparent consequences. Otherwise, the continuing increase in dependency of the financial sector on electronic transactions and machine intelligence certainly makes them more vulnerable to external and internal (even self-inflicted) cyber attacks.”

There will be ‘digital hostages’ and ‘digital colonies’

Chris Uwaje, president of the Institute of Software Practitioners of Nigeria, wrote, “The 21st century will take digital hostages and there will emerge some digital colonies in the very near future. Some nations will wake up from their deep slumber someday—in the middle of the night—to find out that they have been held hostage digitally. Cyberattack may cause a major national blackout and stampede and indeed may lead to a classical civil war—where drones will become a child's play. But with a standardized global peace architecture, there will be some confident-trust pathway for sustainable hope.”

The real threat is long-term infiltration and ‘continuous monitoring’

Clifford Lynch, executive director for the Coalition for Networked Information (CNI) and adjunct professor at the School of Information at the University of California-Berkeley, wrote, “The entire information security situation seems to be totally out of control at this point at every level: individual consumers, businesses, critical infrastructure, military systems. Obviously, the kind and degree of vulnerability varies from sector to sector, but it certainly seems clear that non-state actors of various kinds can cause massive damage. I am also concerned that so much of the thinking seems to be focused on ‘attacks’ and ‘data breeches’ and similar events, as opposed to long-term infiltration of systems, continuing monitoring, subtle data corruption, and the insertion of disinformation, which are at least as dangerous.”

The penultimate and hopeful statements

Rashid Bashshur, senior advisor for eHealth for the University of Michigan Health System, observed, “Hopefully, we will have a better understanding of the causes of massive problems of insecurity in personal safety and cyber safety. Mischief, greed, and hostility cannot be ruled out. But they can, and should be, alleviated. We can't stay dumb forever.”

Fredric Litto, a professor emeritus at the University of Sao Paulo in Brazil, wrote, Yes. “It is very likely; but just as likely is that we will pick ourselves up, rebuild, and continue on our course, just as happened after the Lisbon earthquake, the atomic bombs in Hiroshima and Nagasaki, and the World Trade Center Twin Towers. That type of resilience is something to be proud of.”

And the final, more doleful word

Larry Gell, founder and director of the International Agency for Economic Development (IAED) wrote, “My first job was working for the generals who ran the US Air Force Strategic Air Command. Our protection depends on our strategic rapid reaction to such attacks, and our ability to implement them somewhere at our choosing. What makes you think potential enemies are not thinking likewise?”