The 2014 Survey: Threat level? Cyber Attacks Expected

Anonymous responses by those who answered this survey question

Internet experts and highly engaged netizens participated in answering an eight-question survey fielded by Elon University and the Pew Internet Project from late November 2013 through early January 2014.

This survey question asked respondents to share their answer to the following query:

> *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.) 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.*

Among the key themes emerging from 1,642 respondents' answers were: Internet-connected systems are inviting targets; the Internet is critical infrastructure for nation-states, businesses, transportation, energy, banking/finance, and essential daily life for billions of people; the tools already exist to mount cyber attacks and they will improve in coming years--but countermeasures will improve, too. 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. Major cyber attacks have already taken place, 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. Cyber attacks are a looming challenge for businesses and individuals; certain sectors are especially vulnerable; there are noteworthy divides between the prepared and the unprepared. There is steady progress in security vfixes; despite the 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 in 2025. 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. 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.

Following is a large sample including a majority of the responses from survey participants who chose to remain anonymous in making their remarks in the survey; some are the longer versions of expert responses that are contained in the official survey report. More than half of respondents chose not to take credit for their elaboration on the question (for-credit responses are published on a separate page). They were asked: "Will a major cyber attack have caused widespread harm to a nation's security and capacity to defent itself and its people by 2025?"

> An Internet pioneer with a high level of technical expertise wrote, "The threat has been hyped. After all crime is already a multibillion dollar industry and this is just more of the same."

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."

An associate professor of computer science at Columbia University responded, "Nations are already preparing aggressively for cyber attacks at paranoid levels and spending at the US Department of Homeland Security is already off the charts. We should not add fuel to this paranoia."

A former chair of an IETF working group wrote, "I don't think a major cyber attack against military/defense targets is that likely—though attempts with serious effects will occur. However, the possibility of a major corporation or non-defense government entity being seriously damaged seems high."

A professor at the University of California wrote, "There will be cyber attacks; mostly by the United States government."

A social policy and new technologies researcher wrote, "The Internet is now for the first time coming to a crossroad, where it meets the reverse side of its own fundamental values and premises: the creativity that is based on free and open exchange of knowledge. To prevent major cyber attacks the development of the Internet should quickly undergo a U-turn, which is not likely nor possible."

A global e-learning expert for the United Nations wrote, "The emerging powers will challenge the existing order."

An anonymous respondent wrote, "For every potential attacker, the government is hiring potential hackers to work on its side. I see loads of smaller attacks happening, but nothing that would cause large-scale loss."

An anonymous respondent wrote, "In the last decade attacks have increased in frequency and sophistication. However, recovering has improved even more. This double trend will continue in the next decade."

A retired defense systems executive, electronics and computer engineer, and IEEE member wrote, "No hype here. Cyber warfare conducted by government and criminal agents will easily result in damages exceeding tens of billions of dollars."

The chief scientist at a Fortune 50 technology company responded, "The 2007 cyber attack on Estonia and the Titan Rain attack on the United States suggest there are more to come."

A CEO wrote, "By proportion it will increase, but it will be well countered as technology development accelerates."

An Internet pioneer and longtime National Science Foundation employee wrote, "I'd like to believe that after a few successful cyber attacks, countermeasures will be adopted and widespread attacks will be thwarted. Or not.”

A computer science and security professor and US leader in Internet security, wrote, "It is unlikely this will be major nation-state versus nation-state. It is more likely going to be non-national players or criminal behavior. Hegemony by major players may be part of this too, but it seems unlikely with interconnecting economies and major physical weapon systems.”

A 30-year veteran of software design, testing, and deployment for the US Department of Defense wrote, “The threats can be thwarted. As we move ahead with advances in technology, we will move ahead in the area of securing that technology. It is not beyond our capability to release more and more data, and secure that data. You can't live in fear of moving ahead with scientific advances.”

A network scientist for BBN Technologies wrote, “This is a close call. There are certainly major vulnerabilities in large-scale systems like power grids, transportation controls, and stock exchanges. Attackers could exploit these vulnerabilities if they wanted to. However, I think of these vulnerabilities in rather the same category as nuclear weapons. If a nation-state were to use one, it would be a ‘one-shot’ weapon; international norms about the use of such attacks would change overnight. (So in this regard, the likelihood of nation-state cyber attack is similar to the likelihood of large-scale war, which I regard as low-probability). Non-nation-state attackers have lower levels of resources to establish capabilities for major attack (these are not cheap attacks), and risk attribution and punishment at the hands of state actors if an attack is exercised.”

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 longtime Internet policy expert and open Internet advocate wrote, "There will be many attacks but the consequences will remain minor as ill will is still quite minor, and, in fact is dropping in the world. It won't be because we are more secure.”

The director of an innovation center responded, "Kinetic warfare will remain the more practical form of attack in the medium term. Leaders waiting for a ‘digital September 11’ to spur action on cyber security need to realize that we may instead see a series of ‘digital Oklahoma Cities’ that are severe, but not crippling, attacks which ultimately spur little reform.”

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."

The founder and CEO of one of the Internet's best-known online services wrote, "No, but I'm being optimistic. Some questions need a maybe answer."

An anonymous survey 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."

The CEO of an ISP serving Wyoming, wrote, "Every major player in the Internet spends a significant amount of energy, time, and money fighting against such attacks. The cost of generating attacks will continue to increase and the derived value (disruption, joy of achievement, etc.) will not support the effort."

The CFO for a major Internet company responded, "As threats rise so do prevention and counters."

A distinguished engineer working in networking for Dell wrote, "It's hard to say, but I will take the 'no' on this one. We would have seen significant smaller attacks by now. With the awareness people have now about security issues, I just don't see that happening. Also, tens of billions may not be much money by 2025."

An anonymous respondent wrote, "This has already happened with the documented attacks of the Stuxnet worm and numerous other incidents described in Ron Deibert's book *Black Code*. Many of these attacks have been quite blatant. There is little reason to think that aggressive initiatives by both nation-states and criminal elements will subside. Likely we are in the early stages of an 'arms race' where the weapons are comprised of code and the participants are actively engaged in cycles of measure vs. countermeasure. A nation's defence strategy must now include considerations for 'cyber warfare' as targeted attacks, particularly against economic targets, are already underway."

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.”

An anti-spam and security architect wrote, "The potential already exists and if there is too heavy automation or critical systems without adequately trained manual backstops, things could go far-far wrong before an attacks effects are felt, add social media fake campaigns that already vitiate elections. If an election for a head of state could be successfully rigged in this manner, it is a scary thought.”

A researcher at Tallinn University in Estonia wrote, “Cyber security advancements will continue on the level that will leave all attacks not very destructive. Cyber wars will also focus mostly on cyber intelligence—acquiring information, not causing mayhem.”

A director of networking and applications predicted, “This is the next generation of warfare, for both state and non-state actors. We've already seen precursors with Stuxnet. I think this will accelerate in the future, especially once people discover how inexpensive it can be to launch a significant attack.”

A professor responded, "Given the heedlessness with which major governments, including the United States, have decided already to weaponize both information and digital infrastructure, it is inevitable both that a deliberate attack undertaken to test capabilities will do serious damage and that some of the weapons being created now will have unforeseen or unwanted consequences, possibly because those who are designing them will lose control of them.”

A futurist with the Foresight Alliance wrote, “Some will say that this is already occurring in the form of theft of information—it depends on how you define attack.”

The principal software architect for a large Internet company wrote, “Such an attack has already happened, if by ‘theft’ we include intellectual property.”

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.”

A director at the Georgia Institute of Technology predicted, "A more likely scenario will be repeated localized attacks and minor, though not insignificant, damage to organizational networks. The development of intelligent agents, redundant systems and distributed processing, in developed countries will probably result in rapid load shifting, occasional intermittent outages, analogous to the not unexpected power outages due to summer or winter storms. In developing or conflict ridden areas, though, this might me a more likely occurrence."

A research fellow at the Global Cities Research Institute at RMIT University commented, "I tend to think many of the threats to cyber security, at least on a massive scale, are overstated."

A professor in a school of informatics and computing at a major university in Indiana wrote, "This is probably likely. We already have seen the chinks in the system through Snowden and others. And the massive theft of credit card information at Target shows us that nothing is really safe. Unless we focus lots more attention and expertise to preventing cyber attacks, it is probable that widespread harm is in store for us until we wake up."

A principal engineer for Cisco wrote, "The answer is, 'Yes, but we won't necessarily recognize it as such until much later.' Cyber attacks offer the possibility of achieving a traditionally military objective, like disrupting an opponent's control over natural resources or geographic territory, by non-military means. However, if the objective is to avoid an actual military confrontation, the attack must be non-attributable. So coordinated cyber warfare is likely to include multiple actions designed to cause major economic dislocation and sociopolitical turmoil while appearing to be endogenous: domestic hackers, commercial incompetence, local infrastructure failure, and so forth. Ideally the attacks would lead to regime change, civil war, regional secession, and an inability to sustain military or economic hegemony."

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."

An analyst at a US think tank wrote, "Already there are lots of accidents at chemical facilities—within the decade I bet there will be a deliberate cyber attack on one that results in casualties."

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."

An anonymous respondent who works as the CEO for a technology company observed, "Networks are becoming mobile, more and more resilient, self-organizing, and self-healing. As information flows more and more on decentralized networks, nations are less and less vulnerable to cyber attacks. The complexity of the global network architecture and gigabits infrastructure makes it more and more difficult for a nation to be attacked and taken of the grid."

A private law firm partner specializing in telecom and Internet regulatory issues responded, "Cyber attacks will mainly be Willie-Suttonesque: they will go where the money is. There will be lots of theft from banks and other institutions. But I suspect that terrorists or individual crazies will not be able to launch nation-harming attacks, and at the same time that nation-states will find it in their interest not to do so. Mutually-assured destruction works in the cyber age just as it did in the nuclear age.”

An entrepreneur and electrical engineer active in ACM and IEEE wrote, "A better answer is ‘maybe’ There is certainly a risk. It's also certain that whatever does happen will be inflated in the press (because disasters attract readers and viewers). But $10 billion in damages from one specific incident is relatively unlikely.”

An executive at a top-level domain name operator wrote, “If ‘billions of dollars’ are converted into other local currencies, we may already have witnessed such cyber attacks (i.e. Estonia). When one considers the economic costs a significant storm can have on the nation's infrastructure (with concurrent security implications), a cyber attack in an increasingly inter-connected economy run on bad/poorly safeguarded code is not hard to imagine.”

A research fellow at a top research university wrote, "A combination of flaws left in hardware/software purchased by nation states and other actors and general complacency among consumers and thus no incentive for technology makers to improve security will lay the groundwork necessary for a number of future calamities. I am not optimistic there will be a correction before the public becomes aware of the downsides of commodity electronics manufacturing abroad.”

An anonymous respondent wrote, "We're profoundly exposed. Genuine mitigation and protection will take many years, if not decades. The threat face is enormous; nearly the entire networked infrastructure of the United States and North America. The cost of an attack is too low for someone to not try it—in spite of the threat of retaliation. The only issue is how big it might be. What makes you confident we're not getting hit already?”

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.”

An anonymous respondent wrote, “I think we've just been lucky so far and that at some point a cyber attack will succeed. I just wonder whether it will be ideologically driven in any way or just be done to show that it can be done.”

An anonymous respondent commented, “As the technology capable of causing this kind of catastrophe becomes available, so will the ability to thwart this kind of attack. Governments are focusing efforts on detecting and stopping attacks before they happen. Will there be smaller-level attacks? Absolutely. And these will cause disruption and chaos to our society. However, the large-scale attack that is implied by this question will be stopped by those who are trained to detect them.”

A self-employed digital consultant wrote, “Cyber attacks are a form of war. Wars are diminishing in frequency and severity. Cultural imperialism is the new war.”

An anonymous survey participant who works as a cyber security policy strategist and consultant responded, “No, the costs of tens of billions of dollars come from the payments by financial and energy companies for cyber security services. The real cost of hacking is not nearly as substantial as current estimates suggest. For the loss of intellectual property to actually result in damages, the technology must be effectively implemented. Increased rule of law in China dramatically decreases the ability of intellectual property theft to dramatically effect business, however, defense contractors and militaries may see billion-dollar losses.”

An anonymous survey participant responded, “This is an overblown idea stoked by totally paranoid cyber security 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.”

The president of a center for policy on emerging technologies based in Washington, DC responded, “Our defenses are pathetic compared to the risk, for instance, see electromagnetic pulse threats to the power grid.”

A professor at the University of North Carolina-Chapel Hill commented, “This has been over hyped but it won't take much to cause billions in damage and possibly loss of life (e.g., with micro-trading of securities we could see stock market disasters, automated air or train crashes, etc.). I worry as much about a massive EMF from a sun spot explosion as much as a cyber attack.”

A strategist based in the San Francisco area wrote, “The countries with much to lose are also likely to have the resources to defend themselves. While attacks are possible and likely, the damage should be contained below the level of widespread harm."

A leader at the Network Information Center in Mexico, wrote, “No, but close. There will be some cyber attacks causing millions of dollars of damages, but still no lives.”

A past member of IEEE and ACM replied, “It is highly probable. We rely more and more on automated systems and have not yet understood how security and respect for privacy must be integrated in any system from the initial planning on and at every step.”

A government employee in Europe also involved in Internet-based research responded, “The race will no longer be between the nations for who has the bigger bomb, it will be a race for technology and brains.”

A software research and development professional for a major software organization commented, “There are way too many poorly deployed Internet servers to fix them all by 2025.”

An Internet business analyst wrote, “On the contrary, I believe it's more safe. First, international cooperation against Internet crime will be more fluent after ten years' running. Second, the technology about Internet security will develop to a high level.”

An attorney and partner in private law firm wrote, “Hackers are outpacing business, and government itself is launching cyber attacks. It is only a matter of time before there will be damage to government entities, and it will take less time for there to be billions of losses to companies.”

An Internet researcher and entrepreneur said, "Hard to argue that this hasn't already happened (Stuxnet). But I don't foresee cyber-terrorists detonating nuclear plans remotely. At least I hope not.”

An anonymous respondent wrote, “The Internet was not designed to be ‘secure.’ Many of the devices (such as routers), processes (http) and apps (Facebook) we use are also not secure (e.g., NSA surveillance). Combine this with malicious intent and script kiddies trying to break in, vulnerabilities are discovered and shared. As we move to being more reliant on communications technologies for health, for example, we introduce vulnerabilities that can be attacked remotely. That's just software. Combine with remote-controlled hardware (drones, electric grid, et al.), it seems pretty likely.”

A principal engineer with Ericsson commented, “Cyber attacks have already occurred which caused significant harm to people and/or property. They are only going to increase in scale and scope—and may be a part of what either convinces people to take their privacy seriously, or a part of what ends up locking the entire Internet down into a relatively steady state, either driving the ‘next new thing’ or driving an anti-technology backlash.”

A business school professor commented, “Not at the tens of billions of dollars level. Maybe, but I think it's unlikely. There will, however, be very significant cyber-attacks, doing many millions of dollars of damage. My question is whether we'll ever hear about them. Both the government and major corporations have strong incentives to keep losses from cyber-attacks quiet.”

A university professor wrote, “The United States, China, and Israel are prime candidates and possibly the United Kingdom and Iran. Vulnerabilities include attacks that shut down major surveillance systems and major banking and communications systems. Money could get diverted. There could be communications scares—e.g., fictitious infectious disease outbreaks. Air traffic control systems are also vulnerable.”

A professor at a US research university wrote, “Maybe I have too much faith in the system but I like to think that the safeguards are keeping up with the threats, or that the safeguards will quickly come to the rescue.”

An employee of the US government based in Washington, DC, responded, "Organized crime is probably the most likely to pull off a large-scale cyber attack, and those would likely be targeted strikes on specific banks. A big successful hit would cause a scramble and temporary panic, but not widespread harm."

A PhD candidate in information sciences and technology observed, "The US government investment in cyber security is enormous and likely only set to grow. Coupled with decreasing privacy for regular citizens, it is unlikely that widespread and damaging attacks on the nation will occur by 2025. By 2050? Likely by then."

A media distribution professional commented, "There are too many gifted and educated technology experts to not have the Internet and the electronic side of life attacked. This attack can come from any nation and the victim could be any other nation. As people become more dependent on a life powered by electronics any disruption will cause chaos. A hacker could disrupt power supplies causing blackouts, transportation fatalities, and financial mayhem. Cut down cell phone supply or electricity and communities will be unable to carry out their everyday lives. This attack could be for political reasons, just evil for its own sake, or there is always current problem of credit card fraud and identity theft for monetary gain. What is the financial cost of all crime? How would the world economy be different if crime did not exist?"

An assistant professor at a US research university said, "There will be major attacks and novel ones, but I am skeptical that a crippling/doomsday attack is on the horizon. Not because it's impossible, but because the threats are perceived as real enough that significant resources are being invested and because among those who are drawn to understanding and exploiting security weaknesses, I believe the people who would do widespread harm are not as motivated or plentiful as those who take action to prevent and limit the damage of such efforts."

An anonymous respondent commented, "The level of threat is not higher than the devastation already caused by financial speculation."

A research assistant at the Polytechnic University of Portugal commented, "As attacks grow stronger, so will the people using them for other purposes. While hackers use them to ensure freedom of speech and transparency, with time cyber terrorism will be a greater threat. People will have more computing power, larger broadband access and this may lead to further events of cyber terrorism."

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."

A retired professor wrote, “There will be increasing escalation in the scope of cyber conflicts. As new ways of blocking them are developed, new ways of overcoming or working around them will occur. Increasing distrust of governmental and most other institutions will breed increased grass roots coding among some segments of disaffected publics to attempt to inflict major damage on institutions. Attacks will never be fully thwarted. The quality of basic services like electricity, water, sewer, transportation, and food will continue to degrade and become somewhat like the situations in heavy civil war conflicts. Uncertainty will increase about the availability of essential services on a daily basis.”

A specialist for a government organization wrote, “Systems have been more vulnerable in the past and nothing happened, therefore nothing catastrophic will happen in the future. There will be attacks, but not to the point where a nation cannot defend its self. Whatever breaches happen probably won't come from a major hack attack but someone being careless with data or access—like leaving a machine logged in or a password lying around.”

A professor emeritus of political science commented, “Rogues will have amazing capacities. Aurora and the Connecticut school shootings will become obsolete as cyber attacks replace them.”

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 anonymous respondent wrote, “It's inevitable as it's the new version of warfare whether it is done by nations or criminals or something else.”

A professional writer wrote, “Such an attack is certainly possible. Unfortunately, protective technologies tend to be developed only after the need for them is demonstrated by a dramatic event. That tendencies suggests that such an attack is more probable than not.”

A former executive at a major tech company, and now social entrepreneur, responded, “Connectivity of all elements of nations is and will still be imperfect enough that it will not be possible to bring it down in one attack. Of course, the vulnerability of the nation-state itself is a separate question, and I'm less sanguine about that.”

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.”

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.”

An anonymous respondent wrote, “I'm not a firm believer in digital Pearl Harbor rhetoric. But the politics and innovation in this space is so broken that it will be no surprise to me if sensor networks at a city scale are deployed with inadequate attention to security and privacy and as a result, someone hits these deployments. I don't think it will necessarily result in loss of life, but economic losses will be significant and the rethink we will need at that point about how we manage our technologies and lives will involve a radical change.”

A retired software engineer and IETF participant responded, "Nations will be the primary threats to nations, but corporate spying, espionage, and sabotage will also increase, with the tacit or active assistance of national ‘security’ agencies. Information warfare will become even more prevalent, and social networks will be increasingly exploited to spread disinformation, with significant unrest and even revolution resulting. The vulnerabilities of the various SCADA technologies will be increasingly exploited, and subverted driverless vehicles and robotic technologies used to trigger toxic and biological disasters. Robotic military technologies will be one of the early and most visible targets to be subverted.”

A university professor predicted, “Evil forces will continue to find their way into cyberspace.”

A thought leader and principal at a digital consultancy wrote, “Russia and China are working hard to build up this new capacity. Our global finance and infrastructure is vulnerable. Crypto-currency is gaining interest because of this real threat. There will also be mercenaries groups of the best and brightest. Any system created is a system that will either break down or be hacked.”

A professional designer of technological systems wrote, “Proper terrorism will be carried out through the Internet and nation-to-nation disputes will be vectored through data assaults. To an extent this is already happening, as time goes by it will just become more personal and the implications more damaging to nation economies.”

A management consultant responded, “Despite the very real threats posed by the various vulnerabilities and imperfections embedded in technology solutions, cyber security issues in the public domain are almost entirely a social phenomenon driven by end user naivety and short term ‘commercial’ incentives—freebies and so on. This isn't generally a threat of the dimension proposed in the question and I can't see any significant change to this threat scenario in the near future or even later.”

An entrepreneur and business leader commented, “Though I can imagine ways in which such widespread harm could be caused, I understand that many people run just these scenarios to find vulnerabilities and to secure systems. As long as nations and corporations employ hackers and analysts who can stay ahead of the threat, we can avert the widespread harm. That's a weak system, I suppose, but the question is whether I think an attack will have caused widespread harm, and I don't—because I hope that nations are employing the more clever thinkers than those who would do harm. It isn't a matter of whether “people will try. They will. I just imagine that they won't succeed.”

A professor at Florida State University wrote, “Strategies are being developed to minimize systemic vulnerabilities. This may entail creating firewalled and duplicative networks, and some resources that are isolated from public networks.”

A US government research professional wrote, “I would guess this is possible, but not sure that damage of the magnitude described will be possible.”

A researcher based at Harvard University's Kennedy School of Government commented, “I tend to think our sense of danger is somewhat exaggerated in this area.”

A center administrator wrote, “I don't believe we have significant overlap in infrastructure to be susceptible to a major cyber attack.”

A digital strategist and consultant wrote, “There's currently enough awareness and fear to get safeguards out of development and into practice long before 2025.”

A PhD candidate in the social sciences commented, “These events are rare (see Nate Silver's book *The Signal and the Noise*). However, I'm sure the media will play up a less significant event to make it seem that is cataclysmic.”

A consultant wrote, “While cyber attacks will become more prevalent, they will most likely be used to access information, deny access, or mislead. However, I do not envision a cyber attack resulting in massive loss of life.”

A specialist for the business-to-business sector commented, “Attempts will be made but wide-scale damage across multiple sectors at the same time (financial, security, service) would require a massive, calculated approach that would be very difficult to develop and implement. One sector could be targeted and be damaged, but widespread damage across sectors would be unlikely.”

A director of new product development for mobile and digital wrote, “There will be greater issues we will face by this time; I hope we will have figured out how to lock down computers from viruses and trace the sources so that people are more deterred than today.”

An anonymous respondent wrote, “Monetary losses are more likely than physical.”

A senior product manager commented, “Much of the threat is hyped, because the combination of will, drive to cause harm, focus and skills to do so, access and vulnerability, and then luck to pull it all off—add up to a very unlikely scenario for success.”

A journalist and consultant commented, “Because advances and cyber attacks will occur at increasingly rapid pace, there will not be a major attack as described. There will be many attacks that will be rapidly defeated and then there will be more. It will be techno chess.”

A freelance Internet journalist, researcher, and editor responded, “Such attacks are already going on and so far have been thwarted or contained. Cyber security is paramount and of critical importance, requiring endless enhancements and developments to stay ahead of cyber criminals and terrorists. The only recourse is vigilance.”

A federal government employee wrote, “I have no worries about cyber attacks; our infrastructure has great redundancies and resiliencies.”

A manager for online services commented, “Investment in cyber-security at the national and corporate level will drive security in these areas to new levels that will moderate major threats.”

A political scientist who studies cyber culture, social movements, political violence, and African politics wrote, “I imagine that there will be one major attack on infrastructure, but it will be a tester attack to see if they could. It won't be devastating, more like a poke. Maybe shut down a city's power for an hour.”

A program manager for an international nonprofit organization that promotes access to electronic resources and knowledge in developing and transition countries responded, “Governments and business, as well as people, are paying more attention to cyber security issues, so after a decade everyone will be more prepared and able to identify and stop attacks. An insurance scheme will be extended to compensate for the economic consequences of cyber attacks.”

The director of a nonprofit that protects civil liberties online wrote, “Not in the United States. In spite of the government's protestations, it actually does a very good job keeping us safe. There may be other countries that suffer from infrastructure attacks, but not the United States.”

The dean and provost of a research university said, "Nations will devote greater and greater resources both to offensive and defensive electronic ‘weapons,’ but I don't believe these measures will prevent major damage. The environment appears to be much like the evolution of organisms, which are constantly evolving to evade the measures aimed at them. In the electronic environment attackers will constantly work around defenses, which will constantly be updated to deal with new threats. I don't foresee the kind of mutual threat of destruction that was characteristic of the nuclear age.”

An anonymous survey participant observed, “There are current and continuing-to-be developed tools to protect the safety of entities large and small. Continued vigilance will be required, but it is possible to both protect the integrity of nations and change infrastructures as the populace determines necessary.”

A consumer advocate wrote, "It is not possible, nor will it become possible, to wreak such large-scale harm through purely online attacks.”

The chief executive of one of the key Internet infrastructure organizations responded, "Countries will work together to form a framework to address routine cyber security issues."

The director of a leading foresight organization wrote, "No. There will a continuing battle between vulnerability and determined opponents, with opponents having the initiative and first strike advantage. However, counterattack will continue to hold its own."

A freelance technology writer and editor for leading US publications, wrote, "Again, this answer should be 'probably,' because it sure is possible, but companies and government are not longer asleep to the issue. The good news about the relatively small attacks we're seeing now is they're waking up organizations that thought they could deal with security by clicking a box, and they're moving network and software security closer to a front burner in the enterprise."

A general manager for Microsoft wrote, "Cyber-warfare is already underway (Stuxnet). While infrastructure providers work hard to keep networks safe, there are vulnerabilities, and some form of attack somewhere on the planet seems inevitable."

A senior staff member for one of the leading Internet standards organizations responded, "This is like asking 'will a major electrical power bump cause widespread harm'? No, it will not, because it's a network of power lines with big fuses that would prevent any rippling effect. Today we see denial of service (DOS) attacks but it's always a large number of small machines attacking a few big machines. Big machines don't attack each other."

A principal engineer at Cisco noted, "Arguably that has already happened to Iran. Why shouldn't it happen again?"

A professor at the Georgia Institute of Technology, observed, "It's inevitable that there will be a 9/11-scale cyber attack eventually. I have no idea when it will be, but I'm fairly certain it will happen, or at the very least be attempted. Fortunately, there is a lot of money being poured into preventing that. But at the very least, someone will try it."

An academic computer scientist from Princeton University noted, "Major cyber attacks are possible today, and we are unlikely to prevent them by 2025. Such an attack will happen if a party exists who has the will to carry it out and can hire or acquire the necessary technical expertise. Although this will be rare, it seems likely that this will happen at some point between now and 2025."

The vice president of 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. The banking system is a target-rich environment. There's plenty of evidence that bad actors are hard at work scouting out vulnerabilities and that many/most of them are in relatively unfriendly states."

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."

A law professor and former Federal Trade Commission official wrote, "A serious cyber attack is almost inevitable, notwithstanding concerted and well-intentioned efforts to guard critical infrastructure to protect against such an attack. 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."

A lecturer in human-computer interaction wrote, "An attack is likely, though the target is unlikely to be military as military security will remain a priority. Rather, an attack on essential civilian infrastructure such as water supply, electrical grid, air traffic control, or other system is more likely, probably a part of the system that has been outsourced to a third-party company."

A lecturer in international politics at a European university commented, "No, but I think your definition of a major cyber attack is unimaginative and, based upon our past experience with kinetic attacks, I do think that cyber attacks will feature in international politics by 2025—just not in the way you describe them here."

An anonymous respondent said "It feels like this has already happened in some places, or is imminently close. Nations have huge threats to their sovereignty in the face of surveillance techniques wielded by the most powerful governments that give them a newly skewed advantage, one that surpasses in scale everything that more money, influence, and resources could give. Knowledge is power, and so is data. Whoever controls the data controls a lot."

A deputy director with an organization that studies and analyzes US Homeland Security wrote, "This is a networked world; there will always be the possibility of 'widespread harm.' I believe we will continue to improve our ability to protect. We will continue to be attacked. I believe we will be able to keep the damage in the 'highly annoying' range.

An anonymous respondent wrote, "Hacking will continue, with lots of people impacted through credit card fraud and loss of personal information. Businesses will continue to be attacked and many will continue to have poor security. Attacks will continue but widespread harm is unlikely due to the work of white hats and increasing interest by governments around the globe."

A professor at the University of Illinois-Urbana-Champaign wrote, "I do not believe a major cyber attack will cause loss of life, but I do believe it will cause loss of revenue and certain types of property, depending on the property that is plugged into the matrix/networked."

A lecturer at a university responded, “Unfortunately this is an ongoing concern and will continue to require much work to build secure systems. If not criminal cyber attacks, many services are vulnerable to data loss and power loss caused by the environment, climate change, and storms that have become severe around the globe in the last years.”

An anonymous survey participant responded, ” Yes, the major players may have some degree of protection, but one is not confident about that. Just reflect on Stuxnet for a moment. I shudder to think what that would mean for the US electric grid. What would happen in Chicago if the Metropolitan Sanitary District lost control of the sewage system? What if one sabotaged the financial system in a way that no one could use credit cards?”

The principal sampling statistician at the American Institutes for Research wrote, “Nations will make their security modular so it cannot be attacked all at once. However, cyber attacks will be a problem.”

An anonymous survey participant responded, “It will be an ongoing arms race. As cyber attacks become more sophisticated, so will our defenses against them.”

A professor at a state university in California commented, “There will be terrorist attacks that will shutdown the world's infrastructure.”

An anonymous respondent wrote, “I would not like to see such attacks happen to ordinary people. But they may happen if a small proportion of the population monopolizes capital.”

A knowledge expert and consultant based in Australia wrote, “This is a great unknown. Despite the proliferation of nuclear materials over the last 60 years, we have not had a nuclear weapon used in a conflict. That said, the development of destructive technological capabilities by both state and non-state actors has been intense. And more and more of our lives are supported by networked technologies Will there be a ‘cyber’ 9/11? I'd give this a 50/50 chance.”

An independent scholar wrote, “It's possible. So many idiots put everything online (that is, their power system, water systems). There's already a lot of credit card fraud.”

A data specialist for a public opinion research company commented, “Seeing as how banks and online retailers are routinely compromised today just goes to show that security threats will continue to evolve and be very real. I don't necessarily believe there will be an all-out cyber war between sovereign nations, but society very well may reach a point where one disgruntled employee or sociopath could write a script that would cripple infrastructures.”

An anonymous respondent wrote, “In the past two years alone we have seen tremendous increase in risk and severity of attacks. This leads me to believe that in 11 years a major cyber attack will occur at some point likely sooner rather than later.”

A technology consultant wrote, “The Third World War will start as a cyber war. The power shift has moved to the Asian continent. Power is control over devices.”

The leader of a product-usability consulting firm wrote, “Of course this will happen by 2025, because it has already happened. In 2009-2012 the United States and Israel launched a series of major attacks on Iran's nuclear computer infrastructure known as Stuxnet.”

The digital editor for a very large media organization responded, “I'm sure something like this is inevitable. The how, when and why are the unknowns.”

A strategist responded, “Increased computing power will facilitate hackers to the point that no security wall will be capable of stopping attacks.”

A database configuration specialist wrote, “Cyber security at this date requires human security and the 'wetware' is the weakest part of any system. AI could provide better potential security, but only if designed to evolve. Security is each individual persons' business. How many people have a separate login and password for each of their digital events? Not so many, I think. But that would go a long way towards thwarting large data losses / breaches. How many businesses have redundant and potentially easily isolated recovery centers? Not as many as you would think.”

The executive director of a non-profit wrote, “Cyber attacks are becoming more and more commonplace. Look at the recent theft of Target data and the compromises at NSA. We do not have the political leaders to move ahead with vision. If the current administration is soon replaced, we may have community leaders who can initiate ways to curtail loss of life and theft of property.”

An activist Internet user wrote, “Cyber criminals seem to be ahead of governmental entities in their ability to mine big data for information, and perhaps to sell this information to the highest bidder. Ethics in government and business entities are lacking and will be detrimental to the future of secure information.”

An Internet user wrote, “I don't know how but I fear it is just inevitable. There are always groups willing to hurt others and willing to do whatever it takes to do it.”

The director of operations for a consultancy wrote, “Sure, it's happened already with Snowden and the NSA last year.”

A PhD candidate commented, “The US government itself will not necessarily be the cause of any breaches or vulnerability, but that data/safety may be compromised simply because the government regularly partners with private corporations and universities, creating ample opportunities for sensitive data to be accessed by others, or not properly secured by others.”

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.”

A digital transformation manager for a major technology services company wrote, “I don't think it will be long until a major defense installation is hacked, potentially by a stateless actor. I think the damage will be contained and therefore minimal, but the breach will be very public and create a great deal of anxiety among the public.”

An anonymous respondent wrote, “So much of our infrastructure is woefully out-of-date and seems ripe for disaster. Think of air traffic control as an example. It's been nearly impossible to update such systems given current processes and budgeting. At the same time more and more systems have been moved "on-line" and it's doubtful that those systems are hacker-proof. The battle between hackers and ‘hackees’ will continue and it seems inevitable that those interested in harm will have significant successes.”

A new-media researcher and university teacher wrote, “In the past decade we have witnessed so many cyber attacks and data breaches, yet businesses and nations on the whole still haven't made the necessary investments in cyber security. Given that austerity is still the rage among most developed nations and corporations have skimped on safety and security for hundreds of years, what makes anyone think the status quo will change by 2025?”

The managing director of the consulting division at a major US-based digital company commented, “I certainly hope this is not the case however, we as a country (government and corporations) need to get more proactive in this area.”

A technology developer wrote, “This is already happening. The Chinese and Russians have not made peace—they've just transferred their battlefields.”

An author, communication consultant, and historian wrote, “As generals fight the last war, those responsible for cyber security are fighting the last threat. Furthermore, those responsible for cyber security—both those in the public and private sectors—tend to underestimate the dangers of cyber attacks. A major cyber attack most likely will mimic the 9/11 attacks: the psychological and economic disruption will far exceed the actual damage. Electric utilities, air transportation, stock markets, banking, and communication are among the most likely targets.”

A professional educator wrote, “The key is realizing that anything and everything can be compromised due to a combination of accessibility and motivation. Some people are amoral and immoral: always have been and will continue being such. Acknowledging the human aspect is paramount.”

A lawyer working on technology issues wrote, “Because people trust that their data online is secure, there will be a major cyber attack. Beyond personal security, it is worrisome to have a major threat to archived data—such as that exists with the Library of Congress, etc.”

A university professor wrote, “Probably yes but this is hard to predict. If security redundancy and watchdogs are not supported, yes we have serious problems.”

A consultant responded, “While the US government attempts to stay on top of cyber attacks, only the larger corporations have systems in place for the protection against cyber attacks. Even then, they often don't have the best technology in place. Smaller companies rarely invest in the high tech staff needed for the protection of data, and these are the companies that make cyber attack easy. Other nations may not have the budget requirements for better protection. Since countries 'share' information, it will reduce the effectiveness of any cyber protection that may be in place."

A professor at the University of Colorado wrote, "Utilities, banking, transportation, security, food supplies, and communication are all vulnerable to either physical attacks or cyber attacks. How well we cope depends on whether the response looks like New Orleans or small towns in Mississippi in the wake of Hurricane Katrina. I do not think the level of threat has been hyped—very few people realize the opportunities for disruption. Just investigate the system of transporting water from the Western Slope to the Front Range in Colorado."

A professor of new media at a major university in the United States wrote, "Our banking and financial systems are increasingly vulnerable to criminal attacks due to a lack of cooperative effort to make the systems more secure. In addition, there is a general failure to develop a skill and knowledge base of cyber-security professionals."

A retiree responded, "Would like to think not, but in a world of 8 billion on a planet made for two something nasty is bound to happen."

A retired state government official in the US commented, "I fully expect a major cyber attack earlier than 2025. The country with the greatest ability to control technology will probably be the next great power."

A professor at the University of Pittsburgh commented, "Computerized control of basic physical and social infrastructure creates vulnerabilities that will be occasionally exploited."

A digital consultant wrote, "This issue will follow what happened with the atomic weapons in the era of the Cold War. The different actors (governments, corporations, power groups, international organizations, etc.) will be primarily interested in a catastrophe that will not happen because, as then, would suppose the annihilation of an important part of the world (the size of the country itself does not matter, what matters is the fact itself). No one will be willing to open Pandora's box before the risk of whatever it is backfiring. The balance of forces will impose and seek other goals, such as the space race to create the first colony on Mars or the like."

A technology journalist commented, "I am surprised it hasn't happened yet, but as the world becomes more digital, crime becomes more digital, and security experts aren't keeping up. The damage from the 2008 recession is far more damaging to far more people than the average bomb-in-the-street; a large-scale cyber attack could take down any nation's economy for a decade or more (as some argued happened with September 11th)."

The chief evangelist in Brazil for a global Internet company based in the United States commented, "Only a small number of nations will be properly prepared to counter these cyber attacks. As the world globalizes, local incidents will continue to happen causing small and fast cyber wars."

A consultant to state higher education organizations focused on adult college completion responded, “We need to create full fail-safes or backup environments to allow daily business and activities to continue. If not, cyber attacks could quickly result in chaos and eventual anarchy.”

A retired lawyer and political activist commented, “The level of threat is there and frightening, but also there are talented individuals protecting infrastructure and businesses from it. Every attack that occurs now prepares for protection against the next one—e.g. the Target thefts.”

An anonymous survey participant responded, “The financial system could be affected and badly disrupted. It is a new level of terrorism.”

An anonymous survey participant responded, “As I mentioned earlier, the harder something is to get to, the more adventure and challenge there is in getting to it. There is no foolproof method to protect anyone or anything from attacks.”

An anonymous respondent wrote, “Again, unfortunately, yes. By that time, the measurement will more than likely be in tens of trillions of ‘dollars’ as, the same group of people or their newly indoctrinated puppets will have deflated the value of the ‘dollar with the continuation of a system that allows them to ‘loan’ out the same ‘dollar’ nine times, among other social ploys of a similar nature that are already in place.”

An anonymous survey participant responded, “The United States is apt to have a major cyber attack by 2025. We are continuously increasing the enemies against our current way of life, capitalism.”

An independent consultant replied, “Look at Walmart, with 40 million credit and debit cards hacked. What about the stock market, major banks, and other financial institutions? It is scary what we do not know about our cyber vulnerability. We have become a cyber dependent economy, which places us at risk. Further, we sometimes know the countries of origin for certain attacks, but do not appear—in public at least—to be raising major diplomatic hell with countries like China or Russia. The risk is not over hyped. If the US and Russia can plant a Stuxnet virus, then our own grid and infrastructure is vulnerable. However, I do not believe that the cyber vulnerability is the computer factor; rather I believe it is the human factor and the lack of discipline in our personal habits relating to basic system security.”

A professional who works for a nonprofit social services provider commented, “Attacks on our aging infrastructure are inevitable. We are currently dealing with an antiquated power grid that cannot withstand a hot day without threat of outages. A cyber attack can easily exploit this weakness and cause catastrophic harm by disrupting our electricity for any significant length of time. During Hurricane Sandy I saw firsthand that society would break down much more quickly than we'd like to think. After only two days without power and gas, tempers were high, conspiracy theories were floated, and violence and threats of violence increased with each day. We are already victims of theft of information; it is easily conceivable that hacks can be made to the computers that are used for national defense. There will never be a way to stay abreast of cyber threats to individuals or our country, a simple attack that disrupts communication can create havoc; particularly if it lasts for several weeks. This scenario is becoming more likely to me."

An author and blogger responded, "We are living in a state of denial, just like Californians who refuse to assemble earthquake emergency kits (that's me, actually). We've already seen with Twitter hijackings, credit card and ID theft, as well as other hacks, that evil is alive and well in cyberspace."

A university professor responded, "Hackers do this for their own reasons and purposes. Most of the time they do it to be recognized as 'somebodies.' There are no noble reasons behind these activities. It is pure selfishness! Of course there are incidents happened for profits. If we continue seeing issues related to unequal distributions of wealth, these will happen again and again."

An anonymous respondent wrote, "The recent hacking of Target stores' databases shows just how vulnerable our retail system is to hacking. Banks and securities markets may be next, unless there is adequate failsafe system protection taken."

An anonymous survey participant responded, "The damage will come mostly in the property or money area."

An anonymous respondent wrote, "Of course there will be criminal activities that cause significant harm—but the idea of 'attacking' one country with the idea that one can remain safe is quickly become untenable. We are becoming so interconnected—to harm one country will inevitably cause harm to self."

A social science research supervisor commented, "Clearly there are devious people whose capacity for evil abounds and until better policing and prevention measures are in place the threat remains."

An anonymous survey participant responded, "I think there may be potential for this. Cyber attacks are getting harder and harder to elude, but I think that it's still going to be a war of small advances. As long as the countries advance fast enough they may be safe."

An anonymous respondent wrote, "Unfortunately, yes. There are always ways 'around' an obstacle. These will indeed be exploited. The costs of these encroachments will only be passed on to the consumer."

A writer based at the University of Puerto Rico responded, "It is a possible scenario because there is more dependency on digital services."

A partner at an organization providing voter-based data for political and government communities commented, "The industry of protection will be the largest industry in 2025. Protecting private assets and privacy will keep individuals safe. Government will never get it right."

A professor at Rutgers University wrote, "Think back to 2001, leaving 9/11 out. Think of the hardware and software advances since then. That's the interval we have going through to 2025. And things grow faster at an accelerated pace, over the common unit of ‘year.’ It is almost unavoidable that there will be some big hiccup in our future. This is, after all, how wars may be fought by 2025.”

A business professional commented, “My answer is not yes or no, but very likely—especially if we as a nation do not encourage technology development and keep pace with the rest of the world.”

A consultant for nonprofit organizations wrote, “It will happen in poorer countries that are not investing in cyber security today.”

An information science professional responded, “The attacks will be incremental and the damage primarily financial. There are already plenty of attacks on bank accounts, etc., which happen inside the country. External attacks may be more of the same.”

An anonymous respondent wrote, “It will happen—who would have thought that terrorists would hijack planes and destroy major buildings a la 9/11. This year we have a huge security breach with Target. Something will happen whether it is by thieves, governments, or terrorists—whether for greed or terror.”

A former DuPont electrical engineer responsible for international electro-mechanical product safety compliance wrote, “Such events will have happened by 2025 and they will have had significant effects. However, I believe we will have dealt with them and moved past them. I can see, for example, a major cyber event perhaps affecting the national electrical grid and perhaps another knocking out a vast portion of GPS operation or Internet operation. The financial system will have undergone multiple significant events. I remember when cable was first being delivered to homes, folks figured out how to thwart the interfaces. Better security happened which also got busted. Now the systems in place seem to be pretty immune to such things (now if they can stop the spam emails and phone calls I'd be a real happy person!).”

A worker for a non-profit commented, “As technology gets more incorporated into everyday life, we leave ourselves at risk for a global shutdown. I don’t think we successfully remove a computer from our lives in 2013. I cannot think of one aspect of my life that is not connected to a computer in some way. If there is a major cyber attack there is a real possibility for catastrophic global failure. We are interwoven, connected, run by, driven by, thought for, asked by, and given to, by and with computers. I don't believe that all cyber attacks can be thwarted. Some can; perhaps the ones on the smaller scale. But as people and computers become more technologically savvy and more sophisticated there will be a major cyber attack.”

A freelance writer and communications director for a state government agency responded, “Of course! I have no doubt at all. Our electrical grid, particularly in the Northeast, is vulnerable, as are our nuclear power plants. If international banks and stores, NASA, and the Pentagon can be successfully hacked now, how could anyone think otherwise?”

A market researcher wrote, “Hacking for fun and profit is routinely making the news now. I expect that—whether from internal or external sources—there will be some successful intrusions of governmental and other infrastructure systems. Many of these will be thwarted (and have been—we just aren't being told), but like in any war, the opposition will win at least a few skirmishes.”

An executive director wrote, “Expect our next wars and terrorist attacks to be fought on the digital front as well. Also expect cyber terrorists to create significant havoc, loss of life, and economic impact in the next decade.”

A researcher wrote, “Our nation's security has always been vulnerable with human spies, early radar devices, human error, and political egos. The nation's security will be even more vulnerable with new ways to implement breaches and misjudgment. One cyber attack that I feel may one day disarm us is the storage of our credit card information in databases and the depletion of our assets—just as our enemies took lessons in our airline schools and then got into a cockpit of a major airline intent to crash our citizens into our landmark buildings filled with helpless Americans, those who hate Americans can successfully be employed in a position to cause much damage in many ways.”

A technology risk and cybersecurity expert for a US financial services association commented, “Nations and terrorist groups alike are likely to use cyber attacks as a method of attacking or retaliating. Civil systems are not designed for this level of threat and thus are vulnerable targets. The ability to respond and be resilient is a long-term challenge in an environment where adversaries have access to tools that can inflict significant damage.”

An anonymous respondent replied, “We as a society are not prepared and or secured enough to prevent a major cyber attack. One group of creative programmers with the intent to disrupt the power or communications grid of any first world country and the denizens of that country would denigrate into tribal behavior quite rapidly. What we should focus on is self-reliance within our communities in a way that we can integrate new technology without risking our vulnerability by relying too heavily on easily-disrupted systems.”

A senior administrator at the University of Maryland-Baltimore commented, “There needs to be greater cooperation among governments and industries to share information about threats and protections. The trade-off is privacy in order to achieve this. Unfortunately, this is an area where one can never rest...this is an ongoing, never-ending battle with no perfect protective system.”

A behavioral researcher specializing in design for online government 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."

A postdoctoral fellow and researcher in informatics wrote, "The cyber weapons industry will exit stealth mode pretty soon and become accepted. Hacker corps as well?"

A director of innovation commented, "My impression is that small-scale and exploratory cyber skirmishes are taking place frequently, and could be moved up in scale fast if required. One of my companies recently ran a conference on this which looked at how to protect critical infrastructures with legacy IT systems, such as some power distribution companies and banks."

The chief privacy officer for a US technology company wrote, "They already have."

A professor of political science at the University of Louisville wrote, "Cyber attacks are overhyped. So far no major attack has shut down government facilities. The exception is the Israeli/US attack on Iranian nuclear technology."

An information science professional and leader for a national association wrote, "Again, current trends point in this direction, and the government is throwing giant piles of money at things like stealth bombers instead of at preventing cyber attacks."

A policy advisor commented, "In comparison to what the banks and Wall Street did to the American economy, the threat of cyber warfare is real. I am confident that the military will conclude that protecting us from cyber warfare can be the next 'Cold War' and that it will secure massive amounts of funding to prevent it."

A leader working to implement the National Health Portal of India wrote, "While many governments are adopting e-Governance protocols and systems, many are not aware or competent to thwart the security threats."

A research scientist for Google wrote, "Western countries that are more dependent upon information technology will suffer attacks from non-state adversaries, in much the same way that terrorism arises from non-state entities today."

An Internet professional wrote, "The white hats are losing the battle to the black hats. The distance continues to grow. I don't see a turning point."

An anonymous respondent wrote, "The more we depend on automation the more we are vulnerable to cyber attacks. It might not be a surprise that a computer virus could be responsible for hundreds of thousands of human deaths."

An Internet business consultant wrote, "Most vulnerable will be the electric grid in many countries that have adopted smart meter technology. Banks and nuclear power plants will also be targets of attacks."

A minority rights advocate and media analyst commented, “It won't just be human disruptions, it will be natural ones like sunspots and global warming impacts.”

A researcher for a major US technology company commented, “This is tough to predict. I'm not sure, but I'm leaning towards yes. It would appear that cyber attacks would be just another medium for warfare in addition to traditional land and sea warfare. Whether such an attack would be successful on a large scale is hard for me to foresee.”

The manager of creative services and branding for a worldwide non-profit responded, “You won't have to wait until 2025. Within the next five years, we'll see a major terrorist attack that relies primarily on taking over the digital controls of a utility, construction, or travel system.”

A doctoral student at the Universidade Estadual Paulista wrote, “Cyber attacks will continue and increase but between advances and undeveloped countries as, between rich countries, nations will be much more careful about beginning an open conflict. This will lead to a super sophistication of electronic espionage.”

A senior policy adviser for a major US Internet service provider wrote, “As with gun control, we seem never to have the galvanizing event—despite recurrent major breaches—that force governments and industries to take all the measures necessary to harden systems. This will require unique levels of leadership and cooperation that the political systems of the world seem increasingly unable to produce.”

The principal research scientist at a university-affiliated research center responded, “Far too many critical systems (e.g., power grid stations) are accessible via the commercial Internet and are too tempting a target (whether to state-level actors or script kiddies).”

An anonymous US respondent wrote, “Ironically, as one of the most connected nations in the world, we are more susceptible to cyber attacks than those who likely will impart them on us. I think a concerted effort by a determined opponent can do sufficient harm to a key piece of our infrastructure such that a general panic will ensue which will amplify the attack so as to cause widespread harm. I am thinking about an attack on the banking system or the distribution network of electricity, gasoline, or home-heating fuels.”

A doctoral student at Endicott College responded, “It may very likely be financial and the wide spread harm will be a slow steady creep of mental, emotional, and physical damage.”

A professor commented, “Trying to stop such attacks will be virtually impossible.”

An anonymous responded, “Cyber attacks will become increasingly common, but their damage will not be something akin to what they have been made out to be. Grids will not collapse. Buildings will not topple. Data and corporate interests are at stake. Financial institutions may very well lose significant sums of money and the government may see the collapse of some systems, but I see no reason why these things would go hand in hand with social collapse. Having witnessed the blackouts in the New England in 2003, I have more faith in humanity than I do in government or industry.”

An anonymous respondent wrote, “Actually my answer is ‘quite possible’ as the potential is there. I can easily seeing a criminal enterprise stage an attack on financial institutions in an attempt to steal billions of dollars via market manipulation.”

A technologist working in Internet policy commented, “We don't have a good idea of how to respond to a major attack, and we are not doing the preparation or design work that would be needed to respond to such a thing. We will learn, and suffering attacks will be exactly what will teach us to proceed with a more considered approach.”

A PhD who works in developing ICT policy for social development and democracy commented, “The more data on NATO national security that is digitized, the more data is vulnerable. That's why I think nations who have insufficient knowledge, skills, and infrastructure in this field have high risks of being cyber attacked.”

A professor at Aoyama Gakuin University, commented, “Answering yes or no is quite difficult. Such a major attack would be similar to 9/11—very difficult to predict.”

The president of a German Internet trade association wrote, “Security by design will be there. People will become more cautious to connect old (embedded) system to the Internet. Whenever software companies like Microsoft, Apple, or Google start delivery of operating systems with the highest security switched on by default so that people have to learn to have less security instead the other way around we might be much safer.”

A research fellow at Danube University Krems in Austria commented, “There are many clever minds, and most information is accessible and is accessed by certain organizations (e.g., NSA). It depends who within an organization can access information collected, or who is able to hack into such databanks.”

A researcher at a small Internet consulting firm wrote, “It seems unlikely that the Internet will be immune to such political and economic motivations. Perhaps after a few such damaging attacks diplomacy will overtake immediate greed and treaties will emerge.”

A professor at a major US research university wrote, "Maybe there will not be not the loss of life listed as a potential outcome in the scenario presented to us, but certainly there will be property losses/damage.”

A researcher at a marketing firm doing work in the online privacy space responded, "There have already been some minor instances. For example, the Stuxnet virus in Iran or breaches of government websites that appear to have originated in foreign countries. I don't anticipate any loss of life, but could see financial losses if bank/financial sites are compromised. Even something dramatic enough to shake up the stock market could cause losses in investments.”

A university research fellow wrote, "Banks and government services will go first, and then quality of living tools like streaming TV and library reservations.”

The CEO of a not-for-profit technology company responded, "Well, one hopes not, but it certainly wouldn't be surprising. The US government seems to think irreparable harm has already been caused by employees walking away with hard drives full of state secrets. I would see this as a form of cyber attack, although I'm not sure I agree that it has been harmful to the country in the current instance."

A researcher and graduate student wrote, "It is reasonable to think that an attack could harm a country in the near future because we are becoming more vulnerable as all our financial interactions are now online."

A professor at California State University-Northridge said, "We can wonder who, when, or how, and to what extent they'll be successful—but whether it will happen? Silly question."

A university professor wrote, "If we reach the point that the social fabric has eroded to the point that we start to attack the very infrastructure of sociality and communication on a grand scale, there is little hope. I think I have a bit more hope than that, but I don't have any good reason why."

A research assistant at the University of Hawaii at Manoa commented, "Many of the 'cyber attacks' we have experienced have been in the form of intellectual property theft or are best understood as assertions of free online expression. By 2025, we will have realized that technological solutions (encryption, firewalls, anti-virus software etc.) are continually open to remote exploitation and we will need to have alternative, low or non-tech options for keeping data secure. Rather than creating cyber systems which can be remotely exploited, biological encryption or non-networked medias will be increasingly utilized."

A leader with a major Internet organization in Nairobi, Kenya, commented, "With the increased cyber crime activities, and the use of ICT in almost all industries, there is a strong possibility of a coordinated attack on systems. But the effects will not be monumental as firms are continuously learning from the existing breaches."

A self-employed programmer and web-developer responded, "I really wanted to answer 'yes' but also 'so what?' It's the cost of being a sovereign nation or a corporation; being a nation or corporation is only a means to limit the risk and as technology solves some risks (e.g., makes transport safer by reducing human error), it exposes new, previously not thought of risks (e.g., different types of attack)."

A professor specializing in information studies at the University of Toronto commented, "This is inevitable given global wealth polarization and the increasing disconnect between powerful corporations and a shrinking middle class to the lower class."

A senior policy advisor for an IT-oriented nonprofit wrote, "I think we are less than 10 years away—possibly less than five—from a major catastrophic event causing harm in the financial sector that is going to drive home the urgency of this issue."

An academic researcher commented, "It doesn't seem possible to keep ahead of mischief-makers."

A freelance media artist and university educator in informatics, art, and social activism responded, “The instability of the global telecom system increases with the increase in complexity and usage. It is likely that this general instability will allow cyber attacks to increase in frequency and intensity.”

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 doctoral candidate wrote, "Although a number of cyber protection and security research, programs, and areas are increasing in the United States, an increasing number of outside entities realize the decentralized powers of corporations, organizations, and government leave the United States susceptible to cyber attacks.”

A Syracuse University professor wrote, "There will be several financial fiascos and some major traffic blivets.”

A member of the Internet Society wrote, “If no action is taken at international level on security and protection of access to Internet, a disaster case will certainly be unavoidable.”

An academic researcher at MIT wrote, "This harm in the United States may be caused by another nation.”

A member of the Internet Society chapter in Costa Rica wrote, "I'm afraid that if respect for privacy does not come back to the central issues, yes, we will suffer major attacks.”

The head of a department at a top US university wrote, "This will likely happen at some point—but I am not sure it will be by 2025, or whether it will be widespread.”

An anonymous respondent predicted, “There will be attacks amounted to a few billion dollars perhaps, and some deaths, but nothing crazy unless you consider drone strikes cyber attacks. Sounds more like you mean hacks, which are using technologies against their original purpose. I don't think hacks will account for more than a few billion dollars at a time.”

A researcher and writer working at a major university commented, “Grids are vulnerable, in next twelve years at least one somewhere will be dramatically damaged. Electric, gas, or water will be cut off to a metropolis.”

A self-described “social innovation orphan" predicted, “Nation-states are nearing their end. Wars used to be symmetrical. National boundaries used to be clear. The Internet is global and keeps connected people who are nomadic or refugees. Iran is an interesting possible target, for example. What happens if diaspora are able to reclaim their homelands, not through physical war, but through cyber attack? A nation defending itself and its people are very rarely the same thing anymore. It is *either* defending itself OR defending its people.”

A 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.”

A university professor responded, “What happened in Estonia is a very thoughtful example. The whole state administration was paralyzed for three days.”

An Internet policy expert and advocate for online rights wrote, "Although I do think the level of threat has been hyped, the *potential* for cyber attacks that cause physical damage and potentially threaten lives is real.”

An administrator for technology-focused units in 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.”

An anonymous survey participant wrote, "Cyber attacks are a real threat, and within a decade there will be one major attack with real national consequences. Try as they might, nations cannot defend themselves against all threats—as Anonymous and have Wikileaks shown.”

An anonymous survey participant wrote, "I would hope not but it will depend on how much research and development is put into this area. There is as much risk of this happening as there is of a major natural disaster or other kind of terrorist attack.”

The director of a Web-based journalism project at a major US university responded, "It is frightening to consider, but a significant cyber attack that causes widespread harm is almost inevitable in a society that has become as reliant as we are on technology. Banks, the military, utilities are all vulnerable and, I fear, at least one of them will ultimately become a victim of a successful major cyber attack.”

A professor of law at a US university wrote, "Cyber attacks will come in two forms. The first set will be attacks that cripple information infrastructure, with lost information networks having increasingly devastating consequences as we rely more on these systems. But the root cause of loss from these first attacks might be a simple physical attack or even a natural disaster. The second form of attacks will be those that target information systems. These might be launched by nation states, but I think they're just as likely to be motivated by ideology or piracy. I predict that it will be increasingly hard to distinguish aggressive market competition from information warfare."

The technology director for a major global news provider responded, "This is without a doubt the great terror threat of the future, and we are likely as ill-prepared for it as we were 9-11."

A professor of technoculture at the University of California-Davis predicted, "Not really, as most important things have backups and some safeguards. Minor mischief though will be common."

A CTO and vice president for architecture for a North American network responded, "Stuxnet has shown us this is possible. We will surely see a cyber attack with physical consequences by 2025."

A senior consultant for user experience said, "It seems inevitable. Overall organizations will do well, but someone is going to screw up at the same time a bad-guy gets lucky."

The research director at a technology trade association responded, "Cybercrime and cyber attacks will generally operate along the lines of a long-standing illness, and may act to drain energy out of institutions in an imperceptible form (by distracting corporate personnel). Grand attacks will be rare, but repeated small failures and the effort to prevent harm will remain a constant worry."

A creative strategist wrote, "As we rely on a 'cloud,' and as we have a digital self who has a very strong impact on our real daily life, I guess that killing a digital identity will mean damaging someone's real self at some points. People already commit suicide when they feel harassed online; I guess it can be industrialized as our brains are more and more digital."

A senior researcher at a leading British university observed, "The systems are becoming too complex to secure, and the Chinese in particular are constantly looking for ways to exploit vulnerabilities in the West."

A telecommunications and Internet policy professional who works for a Japanese non-profit semi-academic research center wrote, "By either accident (someone skilled messing about with a system and what they're doing getting away from them, like the original Morris worm), or malevolently with intent to harm, some critical infrastructure will be compromised (power plants, dams, road systems) and costs will be lives and billions of dollars. Cyber attack: North Korea will try something stupid."

A self-employed writer, researcher, and consultant, wrote, "Seems very likely that a concerted effort could crash a stock market, wipe out financial records, or override the controls of a plane."

A lecturer at Southern Cross University in Australia observed, "Attacks will be very hard to contain. While I doubt that sovereignty will be impacted, insecurity in the world's global economic systems will increase."

A Mozilla browser engineer wrote, "Military establishments like to inflate the risks of 'cyber war,' but I predict that most 'attacks' will continue as they have done, if perhaps at a higher rate. Stuxnet is more of the model that will be employed, with quiet, targeted, and hard to detect attacks on high value targets. No doubt, other such attacks are already being developed and deployed without our knowledge. These will generate problems for national defense, but this is merely a natural evolution of the continuing advance of attack and defense technology. One thing is certain: the Internet will be a much more complex animal in ten plus years, with far more advanced defense mechanisms. Participating will require similarly advanced defenses as a matter of course."

An anonymous respondent and Internet researcher observed, "Yes, as connectivity becomes ubiquitous attacks will increase. Perhaps even the next world war will be fought out via cyber attacks on national infrastructure in addition to military attacks."

An anonymous respondent wrote, "It is only a matter of time before some person or group figures out how to severely damage some major bank, stock exchange, and/or national tax system. Humans are pretty bad at estimating the severity of risks they've had experience with, and so much worse at doing so for risks they've never experienced. After something catastrophic happens to one country or institution though, others will learn from its mistake and take appropriate measures to fortify their cyber security battlements."

A self-employed entrepreneur and author wrote, "No such thing as an attack that isn't somehow related to our digital infrastructure."

A technology policy expert wrote, "Of course I don't wish this to happen, but as we continue to move more and more things online and into the cloud, away from mechanical 'press this lever' type actions, we are increasingly more vulnerable, just by default. There are a number of places that seem vulnerable to me (though I am not an information-security person). Things like public utilities, the power grid, phone/Internet backbone, air traffic control, train switching, banking systems, and healthcare facilities. I assume that the folks who are in charge of critical infrastructure are taking all steps possible to avoid hacks and attacks."

A web standardization expert wrote, "This seems inevitable, given the increasing dependency upon connectivity we have. While the military, government, and industry are all hardening their networks against active penetration, a denial of service has severe economic impact in a world where a large portion of the population simply cannot work without access."

An attorney at a major law firm responded, "Once objects are networked they can be hacked. The simplest circuit, a light bulb with a switch, is entirely safe when it is not online. The possibilities for hackers are endless—sticking with the light bulb example, the ability to hack a Phillips Hue and have it flash rapidly enough to cause a seizure is either already here or coming soon. Again, this will be a game of cat and mouse with security and privacy professionals struggling to keep up with an ever-growing onslaught."

The general counsel for an Internet domain name registry wrote, "It would not surprise me. Private enterprises will be better equipped to fend off attacks than governments."

A leader with the Internet Society wrote, "This seems inevitable. Attackers are way ahead of defenders."

An anonymous respondent wrote, "We have already seen thefts of assets totaling high numbers. That's an arms race. Infrastructure can also be targeted, in another such race to outwit the latest way to breach security. I expect attacks on infrastructure will be the way severe damage occurs."

A professor at a major university responded, "If we go to war, then we will experience something catastrophic. If not, then small dramatic episodes will characterize things—probably targeted at high-profile commercial organizations, such as Google. Maybe a terrorist network will organize something too, and that might target government programs."

A college professor noted, "Attack is very likely—if war is desired. Cyber theft has already probably helped level the technological playing field across the globe—and that has probably had a detrimental effect on people in the United States that we don't even know of. It would be very easy to disrupt many people using signal warfare or even simply taking the power grid down—especially where there are extremes in weather and people are dependent on temperature control—and also where people depend upon electricity for life-support. This would leave an infrastructure that the 'winner' could then step right into—once they've cleared out the remaining people. I think Detroit may be a metaphor for this—lots of nice buildings left now that the people find it difficult to live there any more."

An assistant professor at a US university wrote, "As scary and dangerous as a major cyber attack is, this is one area in which nations will be forced to work with one another to avoid these kinds of issues. I would be surprised if this isn't already being discussed in the UN or NATO as a part of strategic planning."

An expert on law, politics, and technology responded, "We have already witnessed a few major cyber attacks. As we are becoming more and more dependent on the Internet as a platform for all daily routines, and as children today use the Internet from their first years, many hold the expertise of harming and damaging online systems. While many will have both the knowledge and the motive to cyber attack municipal, state or commercial platform (such as a bank) it is more than likely that cyber attacks will occur."

An anonymous respondent wrote, "Threats due to 'cyber attacks' (meaning, the exploitation of systems by which unauthorized parties put computers or computer-controlled systems to unintended uses) have always been overestimated and hyped by the entities who would sell us the solution to them, or use them as an excuse to increase their power in the political realm. That is not to say there is not an enormous amount of abuse, fraud, theft of information and intellectual property, etc. But none of this comes to the level of threatening the sovereignty of a nation, for the most part because automated, Internet-connected systems have not yet (and in 2025 most probably will not yet have) proved themselves trustworthy enough to not have a human backstop or, at the very least, an emergency stop facility to take the computer out of the loop."

The director of an entertainment media coalition wrote, “A serious breach is practically guaranteed, as is the subsequent crackdown. The United States isn’t just playing defense here. Consider how the administration very seriously considered a cyber attack on Libya’s air defense network in the lead-up to the NATO engagement. We ultimately decided against it, likely for a combination of reasons: we may not have wanted to be the first country to open the Pandora’s Box of cyber war, and we didn’t have enough time to pinpoint and exploit weaknesses in the Libyan network before airstrikes were scheduled to commence. There were lingering legal questions about whether cyber attacks are considered ‘hostilities’ subject to Congressional oversight within the War Powers Act. It seems reasonable that these questions will soon be answered one way or another. And this will undoubtedly impact the evolution of global information networks, as well as potential mutual escalation in offensive and defensive capabilities.”

An anonymous respondent observed, “The good guys and the bad guys are in a never-ending dance with each other, developing and implementing innovations at what appears to be an increasing rate. It is hard to tell who has the advantage, because the stories are not often told in public. The power grid is vulnerable in many countries and many companies have vulnerabilities that can be exploited. It's just a matter of time.”

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.”

An anonymous respondent wrote, “Major cyber attacks at some point are inevitable despite safeguards. Those attacks likely will be a catalyst for major changes in policy and public as well as private spending to create better solutions.”

A researcher at the University of Southern California wrote, “People in certain poorer countries with inferior cyber security systems may have their bank accounts raided to the tune of tens of billions of dollars—the temptation will be too great to resist, and the execution of this heist will galvanize ordinary folks in the United States to call for tighter security.”

A lecturer and researcher at a large 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."

The chief commons officer for a technology company responded, "This is absolutely inevitable, especially as we push Internet connections into things that used to be analog (water systems, electricity, etc). The designers of the Internet of Things are not focused on security. They're focused on size, battery life, etc. They're going to leave gigantic networks of holes."

An academic leader at major US research university's school of information studies observed, "With increased competition, resources become more concentrated (e.g. fewer banks, each of which has more assets), the potential losses from cyber attacks are getting larger. As entities become more tightly connected, losses can more easily propagate across the entire integrated system. Thus, the system is only as strong as its weakest link. In the face of strong pressures to reduce costs and to use modern financial risk management techniques, many companies and countries are making economically defensible decisions that result in over-exposure to catastrophic, but improbable losses.

An anonymous respondent observed, "What sort of damage to expect depends upon the motivation of the attackers. Do we lump cybercrime with cyber attacks? Is this a question of scale or intention? In terms of capacity to defend against either, it's an arms race—attacks become more sophisticated, but there remains a lot of low hanging fruit for attackers. If the motivation is fiscal reward or if the object is confusion/disruption/terror makes a big difference in planning to avert these."

An anonymous respondent who is a well-known author and academic who also consults on digital education said, "My sense working with CEOs is major cyber attacks are already happening every day, and are rarely talked about for fear is may damage business further. Every multinational, every government, is experiencing these."

The CEO of a professional not-for-profit society responded, "The governments of advanced nations may have the commitment to do what it takes to avoid this, but I fear the profit motive will keep private sector companies from making the necessary investments to thwart cyber attacks. Therefore, we are all vulnerable through our banks, credit card companies, and outsourced government functions such as the electric grid and water supply."

An engineer in a networking company and leading participant in the IETF wrote, "Many of our major infrastructure systems are more vulnerable to cyber attack than to physical attack. Someone will take advantage of these vulnerabilities by 2025."

The policy director for a large US-based technology company responded, "We could see a major cyber attack on the nation's infrastructure before 2025. Financial institutions may also be vulnerable."

An anonymous respondent said, "I don't know whether the forces of evil will triumph over the forces of good. Statistically speaking, there is likely to be a major attack which is successful at some point. But so far the defenses have outwitted the attackers, at least here in the United States where the concentration of economic activity would most likely yield a loss in the tens of billions of dollars.”

A college professor and early Internet policy consultant dating back to ARPANET wrote, “We have daily battles around the world today from cyber attacks on government and private entities. Statistically we cannot stop all and some will occur. As they occur we will learn more about how to protect ourselves, yet it will take a transformation of human nature to cause all people to not sometimes turn to the negative.”

The president of a major international digital rights organization responded, “Yes attacks will take place, though it will be unclear whether the scope of the harm was truly intended. We are learning that one of the greatest dangers of cyber attacks is that the attacker may have little actual control over the attack. This was one of the lessons of Stuxnet.”

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.”

A digital media strategist at a US national news organization responded, "It is inevitable that some country or another will experience a cyber attack that disrupts commerce, transport and/or public safety. It's just a matter of time.”

A US federal government employee whose work involves Internet policy wrote, "No one knows, but it stands to reason. If there is a weapon, someone will use it.”

A professor of ICT and social sciences at the University of California wrote, "We will never really believe in our vulnerabilities until something critical happens. We will discover that the government and large institutions are not as smart or as far-seeing as we think, and thus more vulnerable than we think. Wherever and whenever there are vulnerabilities, *someone* will exploit them. And we will see increasing political instability, which will motivate at least some such attacks.”

The director at a nonprofit focused on innovation, technology, and education responded, "Events like Stuxnet haven't been hyped enough, or other cyber attacks (either engineered by the US government or not) to thwart foreign threats. Perhaps they are too complex for the average person to understand, or the crimes seem justified. People may not realize that other governments can copy the code and use it to attack American interests.”

A technical services director for a consultancy wrote, "I don't have any specific information on this, but there are so many layers of code on code, and so many people who are motivated to find their way through whatever gaps exist, it seems really likely that a creative form of attack will break through and create significant havoc. For all the forward thinking we attempt, there's an awful lot of "fighting the last war" or "closing the barn door after the horse has gotten out.'"

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.”

A program director focusing on ICT standards policy, Internet governance. and other issues wrote, "It's inevitable. If states have that ability—and they do—then non-governmental organizations and actors do as well, and it's only a matter of time before that tool is used against a country and/or its people.”

An anonymous respondent wrote, “Hacking and data infiltration seem to be more common, and our abilities to fight them seem to lack the right sophistication to combat the outcomes. It is probably easier to cripple a country via Internet downtime or other security exploitation than waging war with traditional physical tools.”

An analyst for eBay responded, “Yes, this will be a huge risk if we're not smart about how we protect ourselves and make sure we have back-ups and resources. 'Survivor' skills like how to start a fire without matches or building a shelter with only natural resources are just as important now as they were 200 years ago. Digital survival skills are the same. I don't believe in the scary movies of a massive cyber attack bringing down nations, but I do believe there will probably be a few key attacks that will be big enough to justify the attention, dollars, etc. that need to be applied to prevent a widespread attack from happening.”

An anonymous survey participant responded, “The consequences of retribution is all too simple and most likely more brutal.”

A self-employed technology consultant responded, “Cyber warfare against weapon systems or energy or communications grids. All the stuff of current fiction.”

A CEO commented, “There are so many vulnerabilities in our infrastructure that I can't imagine that someone will not have launched a cyber attack of some sort, likely sooner rather than later.”

A retired management consultant for a large international corporation wrote, “The sovereign responses to vulnerabilities will continue to lag the sophistication of the threats. Increasing resources will have to be directed towards security, resulting in a drag on economic activity (lower growth as compared to a threat-free environment). Consumers will pay for increased security that will be provided by private enterprise.”

An anonymous survey participant responded, “Yes, or maybe no. It's impossible to predict what harms will befall mankind in the next ten or twelve years. In the fifties a lot of money was wasted building fallout shelters. Life was a little scary, but thank God they were never needed. Impossible to predict.”

A consultant to nonprofits and to the government of Washington, DC, wrote, “Because I know more about what is happening at a state and municipality level, I am more concerned about how attacks will harm these jurisdictions. I think the federal government will also be impacted but there seems to be some leadership that can herd the cats. The states can't do this.”

An anonymous survey participant responded, “Our international financial markets are so deeply intertwined with the digital infrastructure that disruption from a serious cyber attack can cause widespread harm within a very short period of time. This does not necessarily mean a threat to national security per se, but widespread panic could easily topple the stock market here in the United States.”

An anonymous respondent wrote, “It seems impossible to secure everything. While this will ultimately happen, I'm not convinced it will happen by 2025. Resources will continue to be spent on things that are deemed ‘high-value targets,’ so I imagine a slow attack on lower value targets that isn't immediately obvious for days, weeks, possibly years. I admit, this is the stuff movies are made of, but the truth is often stranger than fiction. Imagine a rogue nation launching multiple cyber attacks on multiple lower value targets such that they can combine data in a way that gives them competitive intelligence. Combine that kind of attack with others that help them gain monetary resources it didn't previously have. Is it possible for the resources gained in these low level, seemingly harmless cyber attacks, to be combined in a way that would allow a rogue nation to successfully cripple another nation? Doubtful. Even in this scenario I don't think a series of slow cyber attacks like the one I've outlined in my ‘movie scenario’ would ultimately render a nation unable to defend itself and its people.”

A postdoctoral researcher wrote, “Major harm brought about by ICT is a disaster waiting to happen, and I think everybody knows it. The exact nature of said disaster is speculative, obviously, but I expect a wide range of security issues to threaten citizens at both the national and international level.”

An anonymous survey participant wrote, “I'm not the first person to suggest that national borders are going to become less meaningful with the speed at which information, in its numerous forms, will begin to travel and have impact. It is possible we will see battles between nation states trying to retain power in a world where borders take on a different dimensionality.”

An anonymous respondent said, “Some suggest that the power outage in New York and parts of Eastern Canada in 2003 were related to a cyber attack. It's unlikely that major economic enterprises will be able to thwart attacks, with their outdated hierarchies of decision-making and response. The question will be whether the outcomes are merely economic or include loss of life.”

A simulation technologist wrote, “Governments will retain the concentrated power and expertise to successfully defend such attacks. Rogue nations will be marginalized economically if their own resources are spent on such attacks.”

A professor at the London School of Economics commented, “Threats are better thought of as remaining largely traditional in nature. Indeed, it might be argued that with the end of the United States’ unipolar dominance, we may be entering a more recognizable period in international relations, with the focus returning to competition between state-actors.”

A PhD candidate wrote, “Some nations will not make the necessary investments to protect their citizens and customers.”

An anonymous respondent wrote, ”I believe this is hyped; it's fear-mongering, really. Then again, who knows? It's probably time some of the hype turned out to be true.”

A retired PhD responded, “Unfortunately, it is possible that government entities will take the approach of corporate IT folk. Until an attack reaches some 'extreme' they keep quiet about it, and try to clean up. The bearer of bad tidings often does not get promoted. Government entities are holders of data that is valuable to other governments, as well as to corporate entities. If the data is laundered, few questions are asked. To the extent that citizens don't trust their government, there is a greater chance that they are subject to cyber attacks. The government tries to keep things quiet, to engender trust, but things merely get worse. Freelancing individuals will try to do more toward accessing data that might be of use to them in some way. To me, having a refrigerator with Internet connections is not a good idea. Will we have K-cups with data sensors?”

A professor emerita in the graduate program at a research university responded, “I do fear a major cyber attack, but also believe strongly in the capacity of humans to work out answers to their problems.”

A retired professor commented, “The attempts will be made. However, with the Target problem and Snowden leak it is going to force government, business, courts, and the public to put a new approach and awareness in this area. The bad guys are always going to probe to see where we are weak. This alone is gong to create new blue- and white-collar jobs that will move into the military also.”

An anonymous respondent wrote, “Recent developments have eroded already-low levels of trust existed at the beginning of this century. Sovereign powers both benign and terroristic will continue to devote increasing resources to such tools in the interest of furthering their influence and economic control.”

An anonymous survey participant responded, “I believe this may have already happened—we just don't know it (e.g., Blacklist-type activity).”

An anonymous respondent wrote, “We rely too much on technology.”

The Web marketing manager at a major Chicago academic medical center responded, “Stuxnet, anyone? If we can do that, a determined Chinese or Soviet programming group could do the same to us. While corporations try hard to protect data security, there's always a way in.”

An academic administrator and former foundation executive with responsibility for information technology wrote, “Again, investment in infrastructure must include securing our power, water, and food supplies. It seems that some corporations are only just now waking up to the very real threat of cyber attacks. William Gibson saw what was coming long ago—corporate and government security will be in a constant struggle to ward off attackers.”

An information science professional responded, “Someone is going to try the science fiction gambit of using an EMP on some country.”

An anonymous survey participant responded, “It's already happening. This is a national economic security issue, but I see very little awareness of it reflected in statements by our political leaders.”

A digital communications manager commented, “If the word ‘cyber’ were left out of this question, the answer would be clearly ‘yes,’ because then we're talking about even a minor war. Adding online aspects to such wars is already happening.”

The senior manager of digital for a marketing agency responded, “Of course—we will start to see more attacks like the one on Target, and more often. The big losses will come when hackers break into government healthcare files and expose people's social security numbers, health problems, mental health issues, and more, to everybody, or they use that information to blackmail us all or cause more havoc in our lives.”

An anonymous respondent wrote, “While it is difficult to predict attacks of this nature, one fact remains certain, innovation should always go along with security issues. The more complex the Internet becomes, the more complex the security apparatus around it must become.”

A survey research professional wrote, “Some major city will have no electric power delivery during a massive heat wave or cold event. Some Cal Tech students will appropriate the traffic message boards and route all the traffic into the ocean. All the pilots of small aircraft at the annual Oshkosh air show will be cyber-jacked and redirected, causing a global slowing of aircraft to and from the Mall of America. More likely, we will have all the data and nation-states will not share with each other except along treaty lines. First and second nations will be differently equipped to manage food distribution in lean years, shut down pandemics, and distribute educational materials to bring countries onto a common stage of literacy, health, and safety.”

A usability engineer wrote, “I would like to think that society has enough skill and desire to stay ahead of the bad guys but I'm not sure. We can recover more easily from economic attacks, but the threat of attacks on property and people might be catastrophic. We have to be diligent and make sure we have enough skilled and smart people on the side of the good guys.”

An information science professional based in Connecticut wrote, “Yes, probably theft more than human destruction. Just this week, Target was, well, a target of cyber attack. It's just a matter of time before someone cracks the code of a government agency.”

An Internet and society academic researcher commented, “This is already happening due to businesses and governments avoiding deals with companies compromised by the NSA.”

An anonymous respondent commented, “The main goal may be to own the people’s data and destroy it or annihilate all the digital history as well as communication routes.”

A an instructor at a primarily online university responded, “Flame/Stuxnet have already demonstrated states' willingness and ability to attack one another's critical infrastructure, and recent hacks of traffic and train control systems—the widespread vulnerabilities in SCADA systems of all kinds—suggest that it's only a matter of time before a major event takes place.”

A market intelligence analyst for a medical publisher commented, “My pet peeve, I do not believe enough attention has been paid to this vulnerable area. I do think there will be more cyber attacks and if/when any harm people either through sabotage of an infrastructure or financial loss, there will be legal backlash. I could see the European nations along with other developed nations enacting severe penalties for such attacks, like life in prison.”

An information science professional commented, “We are more at risk due to global warming and some massive weather-related incident than we are at risk for a major cyber attack. I guess I feel like there will be some way to shut down a cyber attack before there is significant loss of life or property loss. War is still a real threat to so many people on this planet. I understand that cyber security is important to everyone, because so much of our infrastructure and financial arrangements are facilitated through the Internet. Still, I think war is more destructive to people in other countries, causing loss of life and property, in ways that are nearly impossible to remedy or compensate for.”

An information science professional commented, “It seems that security issues continue to happen without much real effort to manage potential problems. A major event will most likely be needed to affect change.”

A marketing executive working in the high-tech industry since the early 1970s responded, “The risk of such attacks could most certainly occur with a rogue nation or terrorist organization. Several countries of the world are currently capable of such attacks and some believe they have already occurred. It is not that difficult to envision an enterprising hacker who can control cyberspace and either break into computer and network centers and create real havoc. Those risks are real and could involve power grids, defense and missile command systems, the stock market, and financial markets via electronic funds transfer."

A professor at a state university in Minnesota wrote, "My real answer is 'probably.' It's impossible to defend against all threats all of the time."

An anonymous survey participant responded, "I am afraid that too many people are uneducated and unprepared for the damage that a major cyber attack would have on everyday lives. There are too many opportunities for these attacks to happen to stop them today. It will take a concerted effort by IT entities around the world to strengthen against a major attack."

An anonymous respondent wrote, "That is the war—aren't we already fighting it?"

The senior strategic planner at a mid-sized agency commented, "Considering that major corporations (and increasingly, secure government entities) are regularly hacked, it seems logical that hacking will continue to become more sophisticated and a small group of hackers can create significant turmoil with a few small gestures."

An anonymous survey participant responded, "A significant attack of the power grid or Internet backbone will have serious financial consequences, even today. Most utility, phone, and Internet companies need to have a dedicated staff that is constantly looking for attacks and shutting them down as soon as possible. Failure to identify and thwart attacks rapidly will be seen as a sign of incompetence (e.g. Target, 2013). As the number of people who know how to program computers increases, the possibility of attacks increases."

A librarian at an American university commented, "There is a possibility that a massive attack (with massive consequences) will occur. The damages will be more of a financial nature, though."

An information science professional wrote, "Yes. Our power grid, our nuclear plants, our transportation, our stock exchanges, our banks, everything runs on computers. One major cyber attack at one major utility and/or a major international bank would do it."

A self-employed digital consultant commented, "The threat of such attacks will be perceived more as a form of democratic protest when social services fail the communities they serve."

A high-level administrator in the Midwest wrote, "It's inevitable. Those motivated by power and greed will remain one step ahead of those trying to keep systems secure. Nations will have to hire the young and 'techie' and not rely on traditional IT systems. For an example, just look at Healthcare.gov!"

An employee of a large legal services organization responded, "Yes, just ask Target how much they have spent on lawyers and consultants since November."

An anonymous survey participant responded, "It's already happened—ask Target. It's only just begun."

A researcher for a large US-based technology company specializing in understanding user-facing impacts of technology wrote, “Didn't the United States just scale up the battle with China over cyber security and hacking? Isn't that what just happened with Target's point-of-sale systems? Isn't the threat that the NSA poses to privacy already an economic threat to the US technology industry? Our inabilities to comprehend the economic, social, and political impacts of cyber security are already debilitating in important ways. No need to wait until 2025.”

An anonymous respondent wrote, “I feel more vulnerable to my own government spying on me then any other attacks.”

A social media consultant commented, “I don't think officials in power will endorse needed methods to stop major cyber attacks for all entities until something really drastic occurs. They are not listening to all of the sources they could be—globally.”

A self-employed communications consultant wrote, “Offense usually outsmarts defense, at least at first. More complex systems have more holes and vulnerabilities if they are to be open and accessible.”

A university faculty member responded, “Just a matter of time. Since this survey was done before the recent Target episode, this shows it will just be a matter of time.”

A retired journalist commented, “If we can't protect against the mortgage crisis, where the cause was greedy people who made bad assumptions, how can we protect against a cyber attack, where the perpetrators aim to cause harm?”

A higher education administrator responded, “Cyber attacks of all sorts will become the primary battleground for individual attackers, affinity groups, and nations. As we become increasingly reliant on AI, we also will become more vulnerable to these sorts of attacks.”

The owner of an Internet and digital marketing company, “Recent attacks on Target and other large companies show that it can be done. There will always be those who seek to destroy and attack online. From a terrorist or war perspective, it may be cheaper and easier to mount such an attack with people on the inside involved, as compared to using actual weapons.”

The owner of a mobile technology start-up responded, “The opening salvo in a war between technically advanced countries will be a cyber attack. The more integrated the target country is the greater the damage will be.”

The director of corporate development for a major Internet company commented, “It's already happened in small instances (Estonia from the Russians, lots of places by Anonymous, Iran by the United States). Vulnerabilities are everywhere if the 'bad guys' are willing to invest enough to find them.”

A self-employed researcher wrote, “Yes, it can happen. There are too many possibilities.”

An information science professional commented, “This will be the ‘new’ warfare. Reliance on so much electricity, apps, and infrastructure creates vulnerability.”

An author, researcher, and consultant wrote, “Unless major changes are made to the security of conglomerate data collection, I believe our national and individual liberties are compromised. A significantly increased portion of our government budget needs to be allocated to finding new ways to prevent cyber attacks.”

An administrator wrote, “This will take place in terms of an energy/communications/transportation issue—interfere with inventory flows to a major city and there will be problems, interfere with energy transmission and there will be problems, interfere with communications during a natural disaster and there will be problems. Some nations are more susceptible than others.”

A PhD student and Internet researcher wrote, “The harms will be financial. Military and security systems are less likely to be hacked malevolently resulting in major human or property loss.”

The director of market intelligence at a major networking company wrote, “There will be problems, not to the level indicated above, but substantially damaging.”

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.”

A mobile strategist at an education start-up commented, “Cyber warfare will be a huge threat and very unpredictable. The desire to protect the nation from cyber attacks may result in significant personal privacy issues.”

A self-employed content creator and distributor wrote, “This is probably inevitable—we are way behind in cyber protection.”

An anonymous survey participant responded, “I don't believe the threat has been hyped. I do believe that just as there are brilliant people hacking into systems there are brilliant people working on blocking them and creating new methods of securing important and necessary information and resources. Having said that, electronic grids, military defense systems, and financial markets may all be the target of determined attacks. We can hope that our barriers continue to improve, and that we support the work of our technological experts to protect our vulnerabilities.”

A public affairs official for a US federal organization commented, “Well, to some degree we have already experienced this situation with Russia's cyber attack against Estonia in 2007 (effort to bring down networks and compromise command and control ability). From a military perspective, in advance of any formal conflict, the goal will be to first shut down an adversary's network. That's before any attack jets or bombers are in the air or Marines are boarding landing craft for ground presence. Outside of good old-fashioned industrial espionage, I don't believe it's in a country's best interest to launch a damaging cyber attack against another state (let's say, China and the United States as there will be too much economic interdependency). A major cyber criminal attack is probably more likely."

An information science professional wrote, "We are vulnerable and the United States is a target."

A director of research, planning, and evaluation predicted, "Cyber warfare will continue to grow as the mechanisms of war continue to diversify and continue their dependence upon the Internet for their very function."

A retired senior analyst for IT wrote, "The question is close to meaningless for me. We already have such possibilities, and it is the duty of nations to pay attention. Deliberate such attacks mean war. Your scheme reminds me a bad spy story of the fifties, not future events."

A state government library advisor wrote, "Whenever a nation purchases security items from those without allegiance, it can leave that country vulnerable, especially when it is computer based. And, no one can determine true allegiance anymore, especially with swiftly changing political situations. The domino effect can make a small security event a significant one."

A professor emeritus at San Francisco State University wrote, "Based on the cyber attack on the Iranian nuclear program, it is reasonable to assume that eventually there will be a successful cyber attack on the United States and other countries, since cyber warfare is inexpensive relative to 'real' warfare."

A marketer and writer responded, "Hackers are getting smarter, and 'good' people are capable of being turned to help exploit a threat."

A senior project manager in software development wrote, "Our government is busy developing the kind of technology to ensure that these kinds of crippling attacks on vulnerable systems stay a valid option for our own warfare. The problem is (as it always has been) there's no keeping a lid on Pandora's box. A new Cold War involving the development of computer viruses has already begun, and these are not chemical compounds that are easier to patent and contain, but rather ideas and new concepts in computer warfare that anyone can further develop and use, outside our Government's labs."

A director of marketing responded, "Everyone is vulnerable, and I don't see a situation where this isn't a real possibility, especially for countries that may not have as much depth in the area of online security. I also think that as more people move their lives online—photos, videos, financial data, online banking/brokerage, etc., the more opportunity there is for hackers to steal."

A university-based information science professional wrote, "Absolutely. I think the means and the willingness to strike is here already."

A new-media communications specialist commented, "Yes with every brilliant innovation there will be a counter-brilliance trying to undo it. These kinds of attacks will render a crippling blow to individuals, governments, and industry—particularly as we become more and more reliant on it. I think the United States has engaged in cyber warfare on other nations and we will also be a continuing target. There is a lot to be said for things written down on an old fashioned piece of paper and locked in a vault. Anything man creates can be taken down and we are fooling ourselves to believe any large system can never be truly vulnerable.”

The CEO of a mid-sized company that has applied for and will operate many new Internet top-level domains wrote, "I am surprised that the sovereignty of nations is seen as something worth protecting. In fact, I see sensitivities about sovereignty, and the UN-type structures that treasure it, as a major stumbling block to the progress of the Internet and of society generally. As to business, there are many structures that are highly resistant to attacks and penetration: one has only to look at resistance organizations during WWII to understand how to build these. Eventually someone will be smart enough to design organizations in this way, probably after a rather severe security breach.”

An anonymous respondent who works as a journalist said, "Your question implies centralised aggression against a central target. The nature of the Internet and the attacks going on it are decentralised. Together they may add up to big damage. But I don't see how or why one attack would cause ‘widespread harm.’ It will be like ongoing sniper fire rather than a nuclear strike.”

A professor at the iSchool of the University of British Columbia predicted, "The more likely challenging situation in the future will be a massive power outage. Managing against cyber attack is a daily activity. Controlling the weather not so easy.”

An associate professor wrote, "The more cyber attacks we see, the less impact they will have.”

The co-founder of a digital technologies consultancy responded, “This isn't exactly a yes or no question, it is a probability. ‘Cyber attack’ is a hyped cliché, but the vulnerabilities are real. I don't perceive a threat to sovereignty through electronic exploitation. Monetary valuations of damages caused by previous security exploits are clearly exaggerated to serve legal and political interests. An exploit causing loss of life, loss of property, or damage of property is much more likely than an attack whose undisputed monetary impact reaches tens of billions of US dollars.”

A consultant and adjunct professor in satellite systems, wrote, “While the risk is there, all nations and networks are building defenses against such attacks.”

The director for an e-strategies company wrote, "There's a continual dance between the advances on the part of those who intend harm and those who would hope to prevent it. However, I remain an optimist, and I suspect that despite our increasing integration of systems, we will find ways to segregate threats. Which is not the same as a ‘concerted series of attacks working together may cause more widespread havoc,’ but we need to maintain a human link in the chain to prevent cascading damage.”

An Internet law student and human rights advocate wrote, "Sovereign nations in the global north are relatively very well-prepared for any sort of cyber attacks. The story is different when it comes to nations of the global south—where even mediocre, physical security is not a given. The United States, for example, has proven time and time again that it is incredibly well-prepared for such cyber attacks.”

A professor at a major US research university observed, “The government is, for the most part, in defense mode. Even though technology advances, the government is keeping up well enough to be able to prevent such harm from taking place.”

A professor, academic, sociologist, and early Internet scholar commented, “Surveillance breeds more surveillance as fear breeds fear. Security seems the easy answer, but the rat race has only just begun in this area.”

An associate professor at Northeastern University commented, “We are investing a lot of resources in funding security projects and this will help combat cyber attacks.”

An anonymous respondent commented, “I don't think the level threat has been hyped but I think we'll see innovation in detection and prevention systems commensurate with the innovation we see in other areas of technology.”

A leader at Pennsylvania State University responded, “I doubt that this would happen, we are getting better and better as security systems, and while I believe that hackers are getting better and better all the time, I don't believe we'll see that level of loss or damage.”

An anonymous respondent commented, “Well, money on computers is made-up anyway, it doesn't represent anything real, it's, as Baudrillard would say, a simulacrum—so whilst something like that probably will happen, it could be sorted out.”

An information scientist for a non-profit research organization commented, “Attacks will continue to be limited. Offense and defense should continue to improve incrementally. I don't see any sovereign willing to risk harming another nation and causing retaliation, and I don't see non-state actors having the ability to do this.”

An anonymous responder, “I believe that the awareness and investments on security is increasing.”

An anonymous respondent wrote, "I sure hope not.”

A director at a non-profit in Washington, DC, responded, “I expect that there will be a persistent ability of nations and organizations to protect themselves from people who are destructive or inclined to misbehave. Call that a blind faith if you like.”

An employee of an organization specializing in information security education wrote, “Probably not but it might happen. Remember that whatever devious method used can be turned around to attack the attacker so it's to no ones real advantage to have a full scale attack. Even our adversaries would be harmed in that commerce will be impacted and thus their own bottom-line.”

A futurist and Internet activist wrote, “It won't be a problem unless companies don't increase their security.”

The publisher specializing in digital communication wrote, “I'm feeling gloomy but I won't let myself contemplate this one too much. It's certainly possible—awfully possible—but I'm going to dig my heels in and say no just so I can sleep tonight.”

An anonymous respondent wrote, “After the September 11 attack, many companies that had been in the World Trade Center went out of business because they did not have business continuity. They lost all of their data and could not come back up quickly. With the Internet, there are an infinite number of nodes. Data will still pass. My company, for example, uses Google Apps where Google provides our domain's email services for a fee. Their service is 99.999% up. Why would I want to build something that a powerhouse like Google can do faster, better, and cheaper. Then there are Amazon's Cloud servers. I can build a redundant server in the cloud for pennies. Private enterprises like Google and Amazon will remain the citadels of cyber safety.”

An anonymous survey participant responded, “The threats can be thwarted. As we move ahead with advances in technology, we will move ahead in the area of securing that technology. It is not beyond our capability to release more and more data, as well as securing that data. You can't live in fear of not moving ahead with scientific advances.”

A professional educator commented, “Our cyber defense will continue to keep up with and prevent a major cyber attack.”

A PhD candidate commented, “There was the atomic bomb and its permanent threat, and we are still here. Same for cyber attacks.”

An anonymous respondent wrote, “We are aware of the risks—and have taken the appropriate precautions against such an attack.”

A manager for a broadband company commented, “Hopefully by 2025 we'll have figured out how to put the protections in place.”

An information science professional wrote, “Security, against the type of cyber attacks that you envision, is improving every day. I work for a city that takes Internet security very seriously and while it can be aggravating at times to have such tight controls in place, I feel more comfortable.”

An information science professional wrote, “Online companies are always trying to improve their security. I'm not too concerned about it. That's something people value, and I don't think companies will relax on it, but continue to improve it.”

A business professional wrote, “There is a significant threat especially to power grids, police and other first responder networks. However, I think that the public hype overlooks the security measures which will be taken in the next few years.”

A professor wrote, “I wish I could say ‘no’ to this question.”

An information science professional commented, “Mechanical deterioration of public infrastructure will cause an escalating breakdown due to a minor hack into public infrastructure control systems.”

An information science professional wrote, “The cyber attacks on financial institutions will get worse, I believe. Someone who wants to attack will find a way.”

A librarian for the US Department of Education responded, “There have always been intelligence threats and frankly, who knows if there already hasn't been loss of life resulting from a cyber attack" or a hack. I'm sure some spy out there has been compromised and lost other important information that affected our nation. Did something like that happen with 9/11? It's classified and we may never know. Bottom line, there is nothing new here. Whether it's a paper file or a computer file, it can be taken.”

An information science professional commented, “I'm not sure if it will happen by 2025, but a cyber attack is bound to happen at some point.”

An information science professional wrote, “I don't think all parts of our key infrastructure are adequately secured—things like water, power, traffic signals. If they are not secure here—what about more developing nations like China and Latin America. I think over-reliance on technology is a vulnerability to electromagnetic pulse [EMP] weapons and the like. Most people have no idea how to survive without power and Internet and that is a weakness that could be exploited to cause chaos.”

A designer, writer, and web developer wrote, “I fear this is probable and that as a result of attacks of that magnitude, technology priorities will change and (some) balance will be achieved.”

A manager of special projects for a major journal wrote, “I am still not convinced that cyber attacks are fully accounted for in our national security responses. I also see no evidence of real preparation for solar flares or other atmospheric factors that can affect our tech infrastructures.”

An information science professional responded, “The United States and Israel have already demonstrated their capacity to disrupt the Iranian nuclear program through software code. This same approach will inevitably be used to disrupt utilities or other major infrastructures as a means of disrupting economies. Even the ability to disrupt the operation of automobiles by remotely changing the code in circuit boards can have widespread negative impacts on local economies. Creating fear and uncertainty can be a more powerful threat than creating physical destruction.”

An information science professional wrote, “It is only a matter of time before a catastrophic event occurs as a result of cyber-attacks to defense systems, power grids, the water supply, or mass transit systems. I believe major loss of life will result.”

An information science professional wrote, “The possibility exists, as technology and advances continue to be exploited by those with ill intent.”

An information science professional wrote, “This could be very harmful to the way of life expected and lived, and especially harmful to our nation's defenses. Unless more is done for security at personal, business, technology, and national security levels, then unfortunately many levels of security may be harmed.”

An anonymous PhD student and researcher wrote, “This is a double barreled question—I would say ‘yes’ to the first part, a major cyber attack, but ‘no’ to the not-logical consequence of our inability to defend the entire nation and all its people. I foresee perhaps a new cold war in which tit for tat development of encroachments and defenses just play out endlessly.”

An anonymous survey participant responded, “Constant attacks and counter attacks will be the rule. Countries with less sophistication could suffer more but may not be interesting targets.”

A digital information specialist for a nonprofit organization responded, “Eventually a cyber attack will hit something that the harm can't be wiped away. Current attacks on credit card systems can just have the data returned. At some point in time, infrastructure like a power plant will be hit via the Internet and there will be a meltdown. Or someone will lead a Hell Night attack and water will be turned off via an Internet attack or communication systems impacted, preventing first responders from doing their jobs.”

The vice president of a major public association wrote, “I don't think the general public understands the risks and the activities that we engage in that open us all up to significant vulnerabilities. In order to solve for this, either the government or major business groups will need to align their efforts.”

An information science professional wrote, “It wouldn't surprise me one bit. A too heavy reliance upon technology will be society's Achilles heel.”

An anonymous survey participant responded, “I read a book before the year 2000 which used the Gallup poll methods to predict the future threats. So far all of them have come to fruition. One thing the book mentioned was the threat of hackers who could attack medical devices worn on the person, or robots or cars to cause widespread damage and/or loss of life.”

A retired information science professional wrote, “Considering how many breaches of security there are now and how much more dependent on online transactions we are growing all the time, it seems impossible to me that something cataclysmic won't happen soon.”

An information science professional wrote, “Cyber attacks are something we need to guard against. I have to use anti-virus and anti-spyware software. Someone almost wiped out our library's bank account. Some of those people aren't very nice. Instead of airplanes flying into buildings, the harm-causing people use the Internet to steal secret information and to attack computers. Some of those computers are very important and they need to be guarded well. If they are, maybe that major cyber attack will be prevented.”

An information science professional wrote, “I do not have such a bleak outlook with regard to a major cyber attack. I do believe that terrorist groups will continue to try to cause major harm. I think our government needs to stop being ‘politically correct’ with regard to how it deals with terrorists and take the potential for serious threats seriously. Until that happens, I think Americans need to be prepared to live in fear of a serious cyber attack.”

An information science professional wrote, “I'm not sure cyber attacks will be the biggest problem. I'm imagining biological or chemical warfare, natural disasters (so-called ‘Acts of God’), and widespread hunger and disease might pose the most severe threats by 2025.”

A businessperson in the medical technologies sector commented, “There will be damage, but there are sufficient controls in place to prevent a national disaster.”

An information science professional commented, “The majority of businesses and computers have complex systems that are making hacking an impossibility and as they are tested by hackers who work for the government, they will only get tighter, so it would be, in my mind, difficult to launch a cyber attack that could cause major damage. Also, many companies and governments have back-up plans in case of cyber attacks.”

A leadership consultant responded, “Disasters and attacks would have happened by now.”

A marketing research analyst commented, “Similar to the Cold War the major countries and corporations would not harm each other, but rather help protect each other.”

A knowledge-management professional at a large law firm in the United States wrote, “Loss of property through a foreign cyber attack is likely. I doubt there will be loss of life, but believe widespread economic harm will occur within the next five years.”

A digital content strategist responded, “I assume that governments are investing a great deal into Internet security—aiming to stay ahead of the threat of massive cyber attacks. If it does happen, it'll be one government invading the security of another country (i.e. spying) rather than some hackers group or terrorist group. But I think it's extremely unlikely for such a devastating attack to occur. There will be many smaller attacks.”

A digital analyst for a publishing company commented, “For every person that is hacking a system there are people there to defend it. Cyber attacks will continue, but the systems will not be developed so that one hack can completely destroy it. Redundancy systems will be in place.”

A researcher based in Cambridge, Massachusetts wrote, “Such star wars scenarios prove beneficial for movie producers, yet NASA and the NSA have already addressed these issues and will continue to do such in the future.”

A regional sales director for a business commented, “The main job of any country is to protect the homeland—today that also means the virtual homeland and countries will do what the they need to, to protect their citizens.”

A director of computer operations wrote, “I would like to think that if this was going to happen—it would have happened already. Unlike hacking which is akin to terrorism, such a crippling attack would be construed by any nation as an act of war.”

A university-based researcher commented, “It hasn't happened yet and we've had some pretty major leaks already. I think people will continue to be reasonably smart about this kind of thing and will continue to approach warfare in ‘old-fashioned’ ways, or at least more politically appropriate ways. Much in the same way that the Cold War didn't become an all-out nuclear attack—because both sides knew that if they acted, it would be the end of life as they knew it: at worst, everyone would suffer, at best it would usher in a new, more violent age. We're in a technological Cold War that might need some adapting—more enhanced security, for example—but that ultimately won't amount to much.”

A Web designer, developer, and writer responded, “Cyber attacks are a legitimate and often overlooked concern; however, I seriously doubt a cyber attack would harm most developed nations' ‘capacity to defend’ themselves and their people. Hopefully such an attack won't come to pass, but if one does, it might be interesting from a purely psychological standpoint. If a nation's wealth and security can be undermined by stealing some one's and zero's, I think that suggests the wealth and security weren't that ‘real’ to begin with.”

A professional educator wrote, “I think on a somewhat limited basis the Target credit card is a small example of what could happen. Being a hopeful person, it is my thought that safeguards will be put in place to lessen the impact.”

The chief marketing officer for a large agency commented, “No, the threats will only worsen, but the attacks themselves will not have happened on this scale by then.”

A manager for an Australian lobbying organisation commented, “I am confident that most of the world's major economies understand the security threat enough, and have taken steps to protect themselves, that this would not happen. If it happens, it is likely to cause economic collapse in a nation who don't have the resources to understand and mitigate the risks, but I doubt that those nations would allow or could afford non-economic online systems that could affect major assets or lives.”

A research and program evaluation lead wrote, “Security systems continues to evolve in different sectors. The diversity of systems may protect from widespread harm.”

An anonymous respondent wrote, “There cannot be a major cyber attack to actually harm a nation's security leading to big losses and theft towards the general population. Moreover, these kinds of attacks can be stopped by more than one country and collaboration is crucial between countries, between nations to prevent these kind of attacks.”

An associate professor of history wrote, “A massively lethal cyber attack is possible but it probably won't happen. This danger is the equivalent of a nuclear catastrophe: the consequences can potentially be so globally harmful that no sane person or government would initiate such an attack.”

An anonymous respondent commented, “The level of attack will be hyped by some for political advantage. Yes, attacks can be thwarted by prepared persons. Hopefully, groups and organizations will be prepared for cyber attacks.”

An information science professional based in Colorado commented, “While there will always be those misusing technology, there will always be those trained to fight back against any major cyber attack. There is enough paranoia at this time that nations can overcome the problem, unless they were not using regulations to prevent the problem.”

An information science professional at a public university responded, “As long as nations attack nations using cyber attacks (like China), then there will be the threat of wide spread destruction. Since most non-affiliated hackers are interested in money most of all, there will always be the incentive to innovate the best and newest ways to rob individuals and corporations.”

An information science professional commented, “It's already happening. With information stored via Google wallets, apps like Mint, etc., it's very easy to tap into others financial accounts if you have their device. Working in the library, I've seen many phones and tablets left unattended. Telling individuals to keep their devices with them for security purposes does little to deter this behavior. A generation of individuals too trustworthy with leaving devices unsecured, perhaps because it is not the latest and greatest and they feel no one would want it, is very upsetting and will result in major attacks. How? All it takes is the right person's device, access to secure information and a nationwide threat can occur.”

An attorney working on digital and library issues for the federal government responded, “The harm is more likely to be from a commercial attack than a political one. Collapse can best be thwarted by redundancy—the library concept of LOCKSS (lots of copies keep stuff safe). However, that very strategy raises security concerns.”

A retired longtime IT professional wrote, “Terrorists are not stupid. Someone will figure out how to do this. It's far safer than blowing things up.”

An information science professional at a major US school of medicine wrote, “I wish you had a category of ‘maybe’—I guess I think this is more likely than unlikely, so I chose ‘yes’ as my answer. I don't have any rationale for it. I don't really know if the idea of cyber attacks (and my thinking about them) is influenced by media hype or not. But, it seems reasonable to me that it's possible, and that it could have some devastating outcomes. I don't have much else to add to the dialog here.”

An information science professional based in Delaware responded, “It's just a given that as we get better in technology the cyber attackers will too.”

An anonymous respondent wrote, “In the short term we will continue to see cyber attacks on banking and expanding into the public utilities. That will be the most impactful as it will impact everyone who receives that utility. We will continue to enhance air preventive but as they improve, so will the attackers.”

A personal coach, author, and speaker responded, “Your question requires losses and damage at the levels of tens of billions of dollars, Cyber attacks will be against human beings, and I am sure that whoever is counting the toll will not consider the value of human life to be more than a few hundred dollars. Of course if there is theft it will be huge, but it will be done by industry and by politicians who get away with theft every day, carte blanch.”

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 information science professional commented, “There will always be vulnerabilities somewhere that can't be completely closed up, especially since computer systems become increasingly complex. As those systems grow larger, more integral to national security, and more valuable, there will be more incentive to exploit those systems' weaknesses.”

A writer, website operator, and technical consultant for local and wide area networking wrote, “This will happen but it will be incremental rather an explosive event. In fact, this is happening. What was the ‘mortgage crisis’ if not an attack facilitated by available technology that resulted in losses and thefts of billions of dollars that could be credited with certain losses of life?”

A communications manager responded, “It's a worst-case scenario, but certainly seems possible. I don't know enough about data security to talk about the level of threat, but it seems like attacking systems is a very effective way to cripple a company or nation, and we know there are people out there who want to do harm.”

An information science professional in Massachusetts wrote, “This is very likely unless a new technology and a new security industry rapidly develops in order to prevent it.”

An information science professional responded, “Almost any system can be hacked right now and there is likely to be an extreme economic incident in some nation or another. Unless major technology companies and government entities learn to work together, the many diverse systems, the aging of those in charge of the systems, the generational disconnect on both ends (the young without knowledge of the past and the older without technical expertise that is increasing in the younger generation), the systems will be too separate and diverse to be secure.”

A marketing and trend consultant wrote, “Old minds defending critical data against new attack innovations—unfortunately, disaster is inevitable.”

A media consultant, artist, and writer responded, “As an on going problem with escalating outcomes I would be surprised if a major cyber attack did happen.”

An information science professional wrote, “It's certainly a possibility. But I'd like to trust the government is taking appropriate cyber-security precautions and making the appropriate investments in IT infrastructure.”

A leader at a US state environmental agency wrote, “I wouldn't be surprised by an attack that is somewhat smaller than you have described. But an attack of widespread magnitude seems unlikely given the amount of defense in place and the scattered, individual nature of hackers and cyber terrorists.”

An education technology researcher responded, “I don't believe there will be major cyber attacks, but many more smaller ones that will spur policy makers and cyber security professionals to make more investments in this area.”

A higher education technology support professional wrote, “I think that efforts to combat cyber attacks, and to minimize and mitigate the damage have followed fairly closely the ability of cyber attacks to render damage. I suspect that more resources, from the personal level to the national and international level will be put towards protecting against cyber attacks. I expect a large scale cyber attack would have significant financial repercussions within this time frame or even one that might damage our ability to engage in offensive maneuvers for a short time, but not one that would result in loss of life or damage our ability to defend the nation.”

A senior director for digital media responded, “No, I think security will keep up with expanding technology.”

A communications professional commented, “No–this is just pure faith that the United States can stay on top of emerging and harmful technologies.”

A professional who works for a university public health program commented, “All of the threats up to this point have been troublesome but not catastrophic. As security tightens against each threat, new ways to attack emerge, but so far the cyber security industry has not been caught off guard to the point of widespread harm. I think this is also an area that will continue to offer jobs and economic growth in the next decade. Vigilance is the key and that requires resources.”

A government-based program specialist wrote, “This happened just recently with the Target breach and resulted in monetary theft and damages. There will likely be several of these breaches in the future, rather than just one. Hopefully the breaches won't result in a significant loss of life or damage to a nation's security.”

A student at the University of Western Ontario wrote, “Barring human error related accidents, I think that the idea of such attacks are largely the product of watching too many bad American movies. I can see there being small attacks, like the one that happened to Estonia some years back, but I don't see the rhyme or reason for a large-scale attack. Nor the logistical probability.”

An online marketing professional responded, “I can't imagine a cyber attack setting off a missile attack—hoping there are too many checks and balances to allow for that. And such an attack can't cause a tsunami. But an attack on communication systems for air travel, or defense, for example, would be awful. Attacks could probably muck up trading on Wall Street, but I don't see any loss of human life there. Not sure how I feel—this is creating a lot of jobs in one industry, I suppose; folks need to be vigilant and always stay ahead of the next attack. Now an attack that caused Amazon to miss holiday deliveries—that would get attention.”

A user-experience designer for a usability consultancy wrote, “It will take slightly longer than that to create widespread harm, an attack of that scale may be more like 2050.”

A director for research wrote, “It will come in the form of many minor cyber attacks. Little attacks that make small messes and take time and resources to correct.”

An information science professional commented, “This is definitely a threat, and probably a very vulnerable area for even the United States, but I don't see it as causing "widespread harm." People get really nervous about this since so much of our lives are stored online, but I think it is a problem that is overhyped at the moment.”

A retired educational technologies specialist wrote, “Our news media does hype everything. Or maybe I just read too much news. Again, your use of the words 'major' and 'widespread' causes me to answer 'no' to this question. Yes, there will be cyber security attacks as there are now but I don't believe to the level you describe. Smart people and software engineers are already designing to protect rather than be vulnerable to hackers and attack.”

An information science professional said, “Cyber attacks will happen, but not to the degree indicated in the question. The threat level has been hyped because the media is making us aware, but not necessarily in a negative way. We need to be aware that we are not infallible. As technology marches on, so too will our ability to predict or quickly shut down any security threat.”

An information science professional wrote, “This might be faulty logic, but I compare the major cyber attacks with the nuclear crisis of the 1960s and 1970s. It will be (or essentially already is) an arms race, with no country wanting to pull the trigger. Another factor that limits anyone wanting to do such an attack is globalization and how much we are all connected now in terms of products, education, policies, etc. You can't attack one country in an isolated manner without having ripple effects come back and harm everyone, including the attackers.”

An anonymous respondent wrote, “Hopefully by 2025, governments, with the help of IT companies, will have learned how to protect these networks from a mass disaster. Individuals will probably give up more personal freedoms in exchange for protection. It becomes more apparent daily how dependent we are on electricity. If the power grid goes down for several months, due to electronic failure, natural disaster or foreign attack, how will people function and work?”

An anonymous respondent said, “The reality is that the government is in constant pursuit of technology and concepts to outdo anyone who might hack in to the system.”

A professional blogger commented, “Hackers are increasingly political activists and the only effective means of protest against politicians who do not listen to constituents.”

A freelance writer of opinion articles and editorials wrote, “Militant Muslims will do serious damage to basic infrastructure through the power grid or wreak havoc by disrupting financial systems. Government officials will shrug and ask, ‘Who could have foreseen that?’”

A futurist and consultant wrote, “There will be memorable and devastating cyber attacks, but the nature of the networks and usage patterns will prevent them from causing damage at the level of tens of billions of dollars.”

A technical manager who works with professional and financial enhancement tools responded, “Infrastructural disruptions will be more pronounced.”

An information science professional said, “I hope they can be thwarted. And I hope they don't result in large losses of life or damages.”

An information science professional commented, “Attacks can be successfully thwarted by putting hardware and software resources to better use and training people to take fewer risks. I believe the biggest threat is not to organizations, but to untrained individuals.”

An anonymous respondent wrote, “The threat is real but I believe we will be able to defend ourselves against it.”

An anonymous respondent wrote, “Of course this is a possibility and I am perhaps just being hopeful, but, hopefully, most major corporations and governments have been getting the message that this is possible and preparing to offset any negative effects of an attack so it never reaches this point. Our biggest problem is the procrastination of people in government who don't act until after a problem occurs.”

The founder of a public relations firm predicted, “A major US city, perhaps Chicago or San Francisco, will suffer from a major cyber attack from a foreign entity. This will result in more than 10,000 losing their levels since it will occur simultaneously with a natural disaster, further complicating relief efforts. It will dramatically alter the scope and focus of US military defensive posture and preparation going forward.”

An airline digitization consultant wrote, “We'll stay one step ahead of hackers while dealing with cyber attacks that we encounter daily right now. I don't think the United States will become so vulnerable that we can't thwart major attacks, especially as the technology begins to stabilize and it becomes harder to exploit vulnerabilities.”

An information science professional commented, “No, I believe that we are investing a large amount of money in cyber security infrastructure and that this will prevent such a large scale attack.”

An information science professional in Alaska responded, “It's been way overhyped. I also think technology will keep up with hackers. It's getting better every day.”

A gaming, technology, and youth services consultant wrote, “We'll keep on top of security issues and breaches. Also, with robots doing so much for us, and spending so much time immersed in killer apps, people will be happy and less disgruntled.”

An information science professional responded, “I don't think we have enough information today, in early 2014, to figure out what this type of attack would entail.”

An information science professional responded, “I suspect we will instead have a series of less-major cyber attacks.”

An information science professional wrote, “Cyber attacks are just like any other type of attack. People have various reasons for wanting to carry them out and so they will. I don't see it any differently than any other type of attack.”

An information science professional commented, “I don't think it is hyped, I am just hoping we will learn to thwart these.”

A student at the University of Washington wrote, “This is sort of like the cold war. All the big powers in the world have the ability to carry out these attacks, but whoever strikes first will set everyone into a modified sort of nuclear winter. It isn't that the possibility is overhyped or that the attacks can be thwarted, it's that it is too dangerous a tool to use.”

An information science professional wrote, “Electrical and energy grids are run by computers. A cyber attack could cause widespread damage and death to a community. Look at the recent theft of Target credit card users!”

An information science professional said, “I doubt this threat is hyped, I think it's actually larger than the average consumer knows. The bad guys consistently seem to be more motivated and clever than the good guys.”

A metadata expert based in a large US metropolitan area wrote, “First, I was thinking American business and society, but now I'm changing my answer, because I thought about the destruction of Middle Eastern nuclear capacity by Israel and the vulnerability of the American electrical grid. Until more money is put into all kinds of infrastructure that is currently taken for granted, attacks will continue to occur. Even the recent economic attacks on Target and Neiman-Marcus could have been prevented with a more secure credit card system, but I don't really see much willpower going into that area. The United States put more effort into converting the population from analog to digital television!”

An information science professional commented, “We have reason to believe that sovereign nations have already tested this—China briefly rerouting large chunks of Internet traffic through their servers, the virus introduced to the Iran nuclear program. These will continue. I expect that a rogue state or even an independent group will decide that it is worth the risk to do major harm through hacking. Perhaps attack to power grid, or major wiping of bank accounts.”

A media distribution professional commented, “The older software, computers, and networks still in use today by our governments, make our nations vulnerable.”

A director at a major university in Colorado wrote, “This question sounds like a story plot for a movie. Of course, such a scenario could transpire but remember the doomsday predictions of computer disasters from 1999 to 2000. What a bunch of drama that was.”

An information science professional in Virginia wrote, “We get smarter as the hackers get smarter. Each time someone compromises a system we now have teams in place that analyze this and try to see past what happened and determine how to ward off what can happen. One of the few things I do appreciate about the current US president is his willingness to see the need for and fund cyber security research. I don't think this problem is going away any time soon, but with the right funding and people in place it can be stopped and the threat decreased significantly.”

An information science professional wrote, “As the smaller attacks stir paranoia, new safeguards will hopefully come into play. There's always a possibility of something massive happening as we become more and more interconnected, but there is still enough separation to firewall larger problems. If there is money to be made and lost, the incentive for security on that scale is tremendous.”

An anonymous respondent wrote, “The people who are still around looking to attack other nations are renegades and don't have the ability to carry out such large attacks and will still focus on violence as their main tactic, not technological hacking.”

An assistant professor wrote, “I assume there will be several cyber attacks, but I doubt that any will cause widespread harm.”

A survey research professional wrote, “No—hopefully we'll be able to attract, hire, and retain the best and brightest to handle these types of issues.”

A social science researcher and professor studying health information and social media responded, “Major disruptions, perhaps. But we live in an electronic age where money is digits on a computer anyway, so we could recover. Also, a major cyber attack would have to be an incredibly well-organized effort. It's hard to imagine one group being able to carry one out on such a massive scale that would not be shut down quickly. I'm far more afraid of companies controlling my data and the government over-reaching its bounds to police me.”

A professor wrote, “It will be more difficult to find the centralized place for such an attack by 2025. I suspect some smaller such attacks, but decentralized and inefficient structures create their own buffer.”

A research associate and doctoral student commented, “I am an optimist by nature and think that as cyber attacks evolve also protection mechanisms evolve.”

A professor at The New School, based in New York City wrote, “Possible at any point but potentially preventable, just not by taking your shoes of and putting your laptop in a separate bin.”

A social sciences PhD in a research training group at university commented, “There are constant attacks. But, like the millennium bug, a major one sounds somewhat unrealistic to me at the moment.”

A research analyst with a survey research firm wrote, “Threats like bombs, terrorism, war, guns, etc., will continue to pose the real threat to human life. Cyber attacks could substantially affect a nation but not in the ways these events can.”

An anonymous respondent wrote, “The possibility is there, and I'm hoping the government and corporations are taking precautions.”

A digital content advisor wrote, “The biggest threat is to our electrical grid. Hopefully we'll rebuild it before an attack happens.”

An anonymous respondent wrote, “Hackers are already working to disrupt or cripple our systems. It's inevitable.”

The chief operating officer of a large information system wrote, “There is always the potential for vulnerability. Credit card breach is an almost everyday occurrence in spite of the fact that commercial institutions should be on lockdown. Viruses have been known to infiltrate millions of computers. All this will only get worse with greater sophistication. Whether it's an individual reeking havoc for the sheer joy, an individual (group) creating an elaborate breech intending serious harm, or governments themselves infiltrating, this issue is a constant threat. With increased sophistication and increased online or cloud information and data— there is a greater threat with every passing day.”

An information science professional based in Delaware commented, “The more we depend on computers, the more likely such an attack will happen. The success of hackers is a monthly, or even weekly, item on nightly national news programs. I think it would be foolish to not be on the alert and prepared for such an event.”

A self-employed interactive specialist 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.”

The CEO of a consultancy dealing with top-level Internet domains wrote, “I would expect cyber attacks but widespread harm in the tens of billions of dollars are less likely to occur. I could foresee business revenue damages that reach billions of dollars but not property. Mass mobs via messenger, twitters, etc. could occur causing damage and theft but I believe in most first word nations that police and regulatory authorities now have keywords alerting the proper authorities. So it could be prevented, but that of course, depends on whether the authorities have the necessary resources to thwart such attacks.”

A digital communications consultant commented, “I think 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.”

An information science professional responded, “As more of our personal and financial information is housed online terrorists will see the real value in destroying our economy and peace of mind in much broader contexts through technological threats rather than physical ones. Invisible attacks are much more insidious.”

An election commissioner in Kansas responded, “I don't believe cyber attacks are as great a threat to national security as we are led to believe. I do think a cyber attack could take down a major corporation or perhaps industry, collectively perhaps causing tens of billions of dollars in damage.”

The manager of one of the largest public library systems in the United States wrote, “I think that leaders are beginning to understand the need to work together to protect against these threats, but the greater push will be from global industries that stand to lose significantly, such as banking.”

An information science professional wrote, “Hasn't this already happened with the financial crisis of 2007?”

An anonymous respondent commented, “Cyber war is the future. There have already been major attacks, but I imagine that someone will take out a utility, like a power plant or a damn, as most of those services are not in a strict and confined intranet. I believe that because most people don't think about how easy it is to hack, they don't understand why they should be so cautious and so they make stupid mistakes. It used to be that someone had to do something physical like leave a thumb drive in a parking lot and hope it got plugged into a machine, but with tiny computers that are constantly sending and receiving signals, I imagine they will start putting malware into apps, which will transport their nasty viruses to everything with a port.”

An associate professor wrote, “I hope I'm wrong, but I suspect the attack will target financial systems.”

An information science professional commented, “I would hope not. Certainly there could be the potential.”

A director of financial stability for a medium-sized nonprofit wrote, “In the last several days, retailer Target was hacked and customer account information put at jeopardy. So, yes I think this risk will increase especially as people place undue trust in security systems. There will always be individuals (hackers) who will attempt to crack system security if not for financial gain for other reasons. No system is invulnerable to intelligent hackers.”

A PhD and independent researcher said, “I am surprised it hasn't happened yet. My business went into a tailspin a couple of weeks ago due to a malware attack. If one ‘bug’ could do so much, one that hit our systems of online banking, online retail and commercial exchanges, as well as government sites could cause major disruption to society and the economy.”

The digital manager for a hospital and member of the computing professionals' honor society commented, “There's already cyber attacks and security issues, so as we delve even further into technological things, I'm sure loopholes will be found; security will be impaired. I think the level of threat is very real because so much information is digital right now and even more will be in the next few years.”

A director at a research and design firm responded, “This scenario may be a foregone conclusion. Security often lags behind innovations. Our data networks are the foundation of our economic momentum and our communication. I have no expertise to comment sensibly, but it seems a simple financial data heist could top damages over tens of billions of dollars.”

An employee at a US-based, public university wrote, “To clarify, I fear that such an event is possible. I do not know that it is possible, but consider this—would anyone have thought the events of 9/11 would ever have happened? I doubt many did—so, I fear something even more awful may well be possible—and it could be accomplished via a cyber attack.”

An information science professional commented, “As conventional military intervention becomes less feasible for a revenue-deprived federal government, government and corporate interests will turn to offensive cyber weapons to influence or restrict the actions of other nations, businesses, and non-government groups such as terrorists and protesters.”

An associate professor wrote, “The issue of Internet security has not yet had an impact on most people so there is no uproar for government intervention. Until the impact is clear and visible, a major cyber attack is due to occur.”

A freelance marketing and communications professional wrote, “This could happen at any time. Hopefully someone has a Plan B.”

An information science professional wrote, “There is already cyber-warfare, both state sponsored and guerrilla attacks. The United States will lag behind because of the lack of math, science, and technology education.”

An anonymous respondent commented, “The Internet is not secure. Whole countries rely on electricity and batteries. If those go out, huge losses can happen in all economic and social avenues.

People are losing their jobs and their homes; they are angry and desperate. These people are becoming the majority of populations. People will survive any way they can. I would worry about revolutions. We have more and more homeless soldiers trained to fight. Good people being pushed over the edge. Doesn't make sense to me."

An anonymous survey participant responded, "The hype is already out there, crying wolf too many times will make the public immune to the warnings and we will always be in a position of being reactive rather than proactive."

A retiree and volunteer wrote, "This will be the equivalent to the industrial revolution. It certainly caused severe social and economic displacement and disorganization. We're still learning to control it."

An information science professional wrote, "Edward Snowden's low-tech theft of national security information shows that the weakest link is human vulnerability and temptation. Unless we encourage ethical behavior as we gain technical abilities, all nations are vulnerable."

An information science professional commented, "Every system we depend on for the basics—utilities, food, transportation, communication, finance, etc.—now depends on computer technology. We have seen so many presumably secure systems hacked that it is hard to imagine any system being devised that is 100% secure from attack (not to mention internal failure)."

The owner of a creative services group commented, "The truth is that most government systems are not so sophisticated and lacking of efficient interfaces. The Obamacare fiasco is evidence that we are not the Jetsons yet."

An anonymous survey participant wrote, "I would anticipate the security industry—as well as government security activities—to increase and expand during this time span. In fact, I believe we have no choice. Cyber attacks will no doubt be launched, and we as a nation will need to be monitoring security intently at all levels—and forever. It is highly likely some entity will be caught off-guard and be vulnerable to cyber attack. I wish it would not be so, but that would be an unrealistic assessment."

A manager for a major US foundation commented, "Cyber warfare will be the next major line of battle."

A Web technical analyst for a major US county responded, "We have been expecting this to happen for years. Redundancies or safeguards—have not appeared to be that important to business, society, and government today. We are already seeing many vulnerabilities, and the United States also (unfortunately) has a target on it's back from many other countries, including individuals within our own country."

A researcher with a PhD responded, "The Internet is so vast and so vulnerable to interference from states, individuals, and groups, that it's unlikely we won't see some kind of cyber attack within the next decade."

An education consultant, teacher, and developer commented, “Just had a big attack on Target customers. Hackers are probably already at work trying to take down entire systems to create havoc as well as seek wealth. I think they must be being thwarted on a daily basis. Only the imaginations of our current employees in the CIA, FBI, and NSA will protect us. Hurray for them!”

An Internet marketer wrote, “Yes, there are too many people out there that are very well educated and yet have no work. Programming, development, and hacking are things that so many young people have learned and yet they are unemployed in large numbers. This knowledge levels the playing field when they are disenfranchised here and abroad. There are many entities out there that are not a friend of the United States and they will fund activity like this. The NSA spying has probably stopped a lot of cyber attacks already, but on the other hand, having that data collected and stored indefinitely is a huge risk also.”

An information science professional wrote, “While I still remain surprised at the behind-the-scenes investment in infrastructure made by the government to carry out it's massive spying program, I cannot bring myself to assume they have protected resources to the same extent. As we recently saw with the mass theft from Target stores in the United States, people are trying to figure out how to accomplish this. My sincere hope is that it will be an act of revolution aimed at the rich and powerful, but it usually doesn't work out that way. I do think it will be more on the loss of property scale than loss of life.”

An information science professional wrote, “Anything that uses a computer system to work can be hacked.”

A pastor who is active in the Tea Party in the United States responded, “Big banks and military organizations are woefully stupid in anticipating these attacks. Yet I believe they are slowly waking up. Target had a major problem recently. Most Americans don't yet want to believe that our president is a Muslim. Yet the evidence of that is overwhelming.”

An information science professional specializing in business and health sciences wrote, “Sadly, this is all too possible as we try to outsmart ourselves and cyber criminals. The more complex we make things, the easier it becomes to find a flaw or loophole to take advantage and insert malware or worse. Every time we have major spikes in the energy grid, one hears how vulnerable it is to cyber attacks. Consider hurricanes, tornadoes, and major ice storms and the many weeks, months, and years it takes to fully restore all utilities to the impacted region. New Orleans has yet to fully recover its economy after Hurricane Katrina. So, yes, crippling the economy of cities or regions may be an attractive and relatively low personal risk target in the future.”

An anonymous respondent wrote, “In the United States, the utilities grid appears to represent a major weakness. Crashing a major grid and preventing a quick repair will cause major economic damage. Transportation systems are also weak. In Chicago, we had a train appear to operate itself. Could that have been software related?”

A healthcare entrepreneur responded, “I feel that the targets will still be multi-national corporations or governments since they are the easiest to cause material impact. I believe companies and governments will need to strengthen this capability over time.”

An information science professional wrote, “Effective countermeasures will only be designed and implemented reactively, as usual.”

A district software administrator commented, “I can imagine that southeastern Asia and parts of Africa would be targeted first—their infrastructure isn't stable enough to protect against a cyber terror attack of another nation's factories or industries.”

A market researcher for a technology company wrote, “I think this is a real risk, but I also think that we will keep investing in the security needed to thwart these risks.”

A strategy and business intelligence manager wrote, “Although I chose yes, the real answer is maybe. The potential is certainly there as indicated by past attempts. The real questions are—Who is paying attention? What are we doing to prepare for such an attack? Americans are naive enough to believe that the rest of the world loves them because they like American individuals and consume a lot of American pop culture. Most Americans aren't aware that many others don't like American military and economic policies that often harm their way of life.”

A university-based teacher and data scientist commented, “We already see the examples of cyber destruction. We must allow or compel organizations to improve cyber security software, both individual software applications and coordinated systems.”

An online news producer commented, “You do not have to wait for 2025.”

A professor of information systems said, “There are three kinds of vulnerabilities: SCADA, the credulity (or stupidity) of users, and the greed of large companies' leaders. Tepco is only the beginning.”

A digitization manager wrote, “Seems inevitable that as more infrastructure goes digital, more people will have the know-how and desire to exploit it.”

A writer, author, and journalist, responded, “The national grid is completely unsecured, despite statements by government officials to the contrary. I believe the statements are made because they really have no understanding of how to secure the grid. As military and government use of the Internet continues to rise, the question of security is not well addressed. By 2025 there will be many more people able to take advantage of that lack of security and false confidence. Terrorists and others are finding out that the way to cause great harm, both monetarily and risk of human life, is best accomplished through cyber attacks.”

The managing director for a large advertising and marketing agency commented, “Cyber warfare is real and on-going today. State actors will continue to use Stuxnet and other tools to disrupt, delay and destroy enemy infrastructures or demonstrate intent. Non-state entities will master this and attack state players. By 2025, a private-government coalition should have developed sharing tools and protocols that can better protect us. This may require significant international cooperation or proactive action by NATO or other existing multinational entities."

A consultant responded, "The criminals are just as smart and innovative as the rest of us. The continued economic inequality will push people in the direction of criminal activity as legitimate ways of making a living wage diminish. The continuing conflicts over diminishing global resources will also be a factor as terrorist groups of all kinds seek the means to stay one step ahead."

The program manager at a global advocacy organization wrote, "Didn't we see Russia possibly attack Estonia a few years back? Someone took out their telecommunications network, or at least their emergency system. Also there was Stuxnet. This is already happening."

A senior web designer commented, "I fear it will take a significant event like a breach of some vital utility, such as power or water delivery, to make countries take the threat seriously. It usually happens that we need a wake up call that results in catastrophic failure before we all begin to believe it can happen to us."

A government-based cultural technology research analyst commented, "I wouldn't be surprised to see some sort of cyber attack on a major city's infrastructure. I certainly hope that there aren't vulnerabilities, and perhaps there are people working on cyber attacks already, but security has stymied them. In the meantime, nature has managed to do more than enough widespread harm."

An information science director at the federal branch commented, "We have faced this already. Technological developments and innovations are far ahead of legislative and international agreements."

An information science professional in rural eastern Washington State wrote, "We're actually seeing this now. Our cyber infrastructure is vulnerable as is the analog infrastructure that it depends on—electricity and pipeline. We will see a major crippling attack—very likely, more than one."

An information science professional based in Delaware commented, "The risks have not been hyped necessarily, but this race to cyber attack other countries will escalate incrementally giving time for all parties to get better at what they do so that they can attack or defend in a new way the next time. Yes, it will be a dangerous game, not unlike programing drones to kill people remotely."

A University of Missouri assistant professor 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."

The manager of a non-profit wrote, "The recent hacking of Target customers information shows how at risk we are and how evil some can be."

An information science professional commented, “We are very vulnerable. The recent Target breach proves that. I don't think it will be an act of terrorism or war. But thieves will find a way to prove that our system is not up to par. My hope is that we invest the time and money to stay smarter.”

An information science professional responded, “There are so many levels that electronic information can fail or be destroyed. Fail-safes must be devised and employed.”

A research librarian based in Australia commented, “I don't think we understand the vulnerabilities. For example, in Australia one of our two major mobile phone carriers and one of the major power-supply infrastructure companies are both owned by the sovereign wealth fund of another country. In both cases, a cyber attack, either under the auspices of that country or another actor, would have huge consequences for the country. Trade, economic power, and communications, these are global already. The GFC showed how problems in one economy can travel around the world very quickly. We don't understand (at the common level), how these systems are controlled, managed, influenced, and therefore destroyed.”

An information science professional wrote, “There will always be someone looking to break the system, and it is highly likely that someone within the system with the skills necessary to wreck havoc will choose to defect or make a statement by disrupting systems as much as possible, unless we are very proactive in establishing security standards and protocols.”

An information science professional based in Berkeley, California, wrote, “Look, if we can cause widespread harm without digital technologies, we can also do it with digital technologies. The harm we allow ourselves to commit against one another is not a matter of technology but of politics and humanity. We've had war and destruction on a large scale in every era of technological development and I don't expect that the next twelve years will be so different. PS—Our public sector isn't doing nearly as good a job keeping up with digital security as the private sector is doing with digital innovation. This is not a good sign.”

An information science professional wrote, “Just look at the whole Target (online security) debacle. Nothing is safe with the Internet and computers.”

An information science professional responded, “The vulnerability is there, and it's just a matter of time before it is exploited. I would expect that a dramatic event of some sort would set the stage for increased invigilation by the government, all in the name of protecting our freedom.”

An information science professional commented, “I cannot imagine that nations and major economic enterprises have no one on their side who is capable of anticipating and defending against their opponents. That would presume that all of the most intelligent and capable hackers are on the side of evil.”

An information science professional wrote, “Security being what it is today, will only increase. The system(s) will monitor and protect. They need to.”

A retired information science professional observed, “A Rutgers 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.”