## Impact d

### No threat of large-scale cyber-terrorism---30 years of empirical evidence proves

Sean Lawson 11, Ph.D. Department of Communication University of Utah "BEYOND CYBER-DOOM: Cyberattack Scenarios and the Evidence of History" Jan 11 mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history\_1.pdf

Despite persistent ambiguity in cyber-threat perceptions, cyber-doom scenarios have remained an important tactic used by cybersecurity proponents. Cyber-doom scenarios are hypothetical stories about prospective impacts of a cyberattack and are meant to serve as cautionary tales that focus the attention of policy makers, media, and the public on the issue of cybersecurity. These stories typically follow a set pattern involving a cyberattack disrupting or destroying critical infrastructure. Examples include attacks against the electrical grid leading to mass blackouts, attacks against the financial system leading to economic losses or complete economic collapse, attacks against the transportation system leading to planes and trains crashing, attacks against dams leading floodgates to open, or attacks against nuclear power plants leading to meltdowns (Cavelty, 2007: 2). Recognizing that modern infrastructures are closely interlinked and interdependent, such scenarios often involve a combination of multiple critical infrastructure systems failing simultaneously, what is sometimes referred to as a “cascading failure.” This was the case in the “Cyber Shockwave” war game televised by CNN in February 2010, in which a computer worm Leaked U.S. diplomatic cables published by WikiLeaks.org seem to corroborate this accusation (Shane & Lehren, 2010).5 spreading among cell phones eventually led to serious disruptions of critical infrastructures (Gaylord, 2010). Even more ominously, in their recent book, Richard Clarke and Robert Knake (2010: 64–68) present a scenario in which a cyberattack variously destroys or seriously disrupts all U.S. infrastructure in only fifteen minutes, killing thousands and wreaking unprecedented destruction on U.S. cities. Surprisingly, some argue that we have already had attacks at this level, but that we just have not recognized that they were occurring. For example, Amit Yoran, former head of the Department of Homeland Security’s National Cyber Security Division, claims that a “cyber- 9/11” has already occurred, “but it’s happened slowly so we don’t see it.” As evidence, he points to the 2007 cyberattacks on Estonia, as well as other incidents in which the computer systems of government agencies or contractors have been infiltrated and sensitive information stolen (Singel, 2009). Yoran is not alone in seeing the 2007 Estonia attacks as an example of the cyberdoom that awaits if we do not take cyber threats seriously. The speaker of the Estonian parliament, Ene Ergma, has said that “When I look at a nuclear explosion, and the explosion that happened in our country in May, I see the same thing” (Poulsen, 2007). Cyber-doom scenarios are not new. As far back as 1994, futurist and best-selling author Alvin Toffler claimed that cyberattacks on the World Trade Center could be used to collapse the entire U.S. economy. He predicted that “They [terrorists or rogue states] won’t need to blow up the World Trade Center. Instead, they’ll feed signals into computers from Libya or Tehran or Pyongyang and shut down the whole banking system if they want to. We know a former senior intelligence official who says, ‘Give me $1 million and 20 people and I will shut down America. I could close down all the automated teller machines, the Federal Reserve, Wall Street, and most hospital and business computer systems’” (Elias, 1994). But we have not seen anything close to the kinds of scenarios outlined by Yoran, Ergma, Toffler, and others. Terrorists did not use cyberattack against the World Trade Center; they used hijacked aircraft. And the attack of 9/11 did not lead to the long-term collapse of the U.S. economy; we would have to wait for the impacts of years of bad mortgages for a financial meltdown. Nor did the cyberattacks on Estonia approximate what happened on 9/11 as Yoran has claimed, and certainly not nuclear warfare as Ergma has claimed. In fact, a scientist at the NATO Co-operative Cyber Defence Centre of Excellence, which was established in Tallinn, Estonia in response to the 2007 cyberattacks, has written that the immediate impacts of those attacks were “minimal” or “nonexistent,” and that the “no critical services were permanently affected” (Ottis, 2010: 72). Nonetheless, many cybersecurity proponents continue to offer up cyber-doom scenarios that not only make analogies to weapons of mass destruction (WMDs) and the terrorist attacks of 9/11, but also hold out economic, social, and even civilizational collapse as possible impacts of cyberattacks. A report from the Hoover Institution has warned of so-called “eWMDs” (Kelly & Almann, 2008); the FBI has warned that a cyberattack could have the same impact as a “wellplaced bomb” (FOXNews.com, 2010b); and official DoD documents refer to “weapons of mass disruption,” implying that cyberattacks might have impacts comparable to the use of WMD (Chairman of the Joint Chiefs of Staff 2004, 2006). John Arquilla, one of the first to theorize cyberwar in the 1990s (Arquilla & Ronfeldt, 1997), has spoken of “a grave and growing capacity for crippling our tech-dependent society” and has said that a “cyber 9/11” is a matter of if, not when (Arquilla, 2009). Mike McConnell, who has claimed that we are already in an ongoing cyberwar (McConnell, 2010), has even predicted that a cyberattack could surpass the impacts of 9/11 “by an order of magnitude” (The Atlantic, 2010). Finally, some have even compared the 7 impacts of prospective cyberattacks to the 2004 Indian Ocean tsunami that killed roughly a quarter million people and caused widespread physical destruction in five countries (Meyer, 2010); suggested that cyberattack could pose an “existential threat” to the United States (FOXNews.com 2010b); and offered the possibility that cyberattack threatens not only the continued existence of the United States, but all of “global civilization” (Adhikari, 2009). In response, critics have noted that not only has the story about who threatens what, how, and with what potential impact shifted over time, but it has done so with very little evidence provided to support the claims being made (Bendrath, 2001, 2003; Walt, 2010). Others have noted that the cyber-doom scenarios offered for years by cybersecurity proponents have yet to come to pass and question whether they are possible at all (Stohl, 2007). Some have also questioned the motives of cybersecurity proponents. Various think tanks, security firms, defense contractors, and business leaders who trumpet the problem of cyber attacks are portrayed as selfinterested ideologues who promote unrealistic portrayals of cyber-threats (Greenwald, 2010)

### No desire for terrorists to carry out cyber attacks---their operations will be small-scale

Spencer Ackerman 11 is an American national security reporter and writer for the Washington Independent "Pentagon Deputy: What if al-Qaeda Got Stuxnet?" Feb 15 www.wired.com/dangerroom/2011/02/pentagon-deputy-what-if-al-qaeda-got-stuxnet/

Points for imagination here: at the RSA information-security conference in San Francisco, Deputy Defense Secretary William Lynn worried aloud about a terrorist group getting ahold of a malware tool like Stuxnet. Sure, al-Qaeda hasn’t launched any cyberattacks so far. Nor have its operatives manifested any ability to design anything as sophisticated as the Stuxnet worm. “But it is possible for a terrorist group to develop cyberattack tools on their own or to buy them on the black market,” Lynn, the Pentagon’s point man on cybersecurity, warned on Tuesday. “As you know better than I, a couple dozen talented programmers wearing flip-flops and drinking Red Bull can do a lot of damage.” Maybe so. But in last week’s congressional mega-hearing from the nation’s intelligence leaders on threats facing the country, no spymaster assessed that al-Qaeda was looking to launch a giant cyberattack. The most likely forecasted method of terrorist assault against the U.S. are “small-scale attacks” like homemade bombs, Director of National Intelligence James Clapper told a House panel. al-Qaeda appears more focused on making inroads to unsuspecting Muslim youth through social media.

### One in three billion chance of nuclear terrorism

John Mueller 10, professor of political science at Ohio State University, Calming Our Nuclear Jitters, Issues in Science & Technology, Winter2010, Vol. 26, Issue 2

In contrast to these predictions, terrorist groups seem to have exhibited only limited desire and even less progress in going atomic. This may be because, after brief exploration of the possible routes, they, unlike generations of alarmists, have discovered that the tremendous effort required is scarcely likely to be successful. The most plausible route for terrorists, according to most experts, would be to manufacture an atomic device themselves from purloined fissile material (plutonium or, more likely, highly enriched uranium). This task, however, remains a daunting one, requiring that a considerable series of difficult hurdles be conquered and in sequence. Outright armed theft of fissile material is exceedingly unlikely not only because of the resistance of guards, but because chase would be immediate. A more promising approach would be to corrupt insiders to smuggle out the required substances. However, this requires the terrorists to pay off a host of greedy confederates, including brokers and money- transmitters, any one of whom could turn on them or, either out of guile or incompetence, furnish them with stuff that is useless. Insiders might also consider the possibility that once the heist was accomplished, the terrorists would, as analyst Brian Jenkins none too delicately puts it, "have every incentive to cover their trail, beginning with eliminating their confederates." If terrorists were somehow successful at obtaining a sufficient mass of relevant material, they would then probably have to transport it a long distance over unfamiliar terrain and probably while being pursued by security forces. Crossing international borders would be facilitated by following established smuggling routes, but these are not as chaotic as they appear and are often under the watch of suspicious and careful criminal regulators. If border personnel became suspicious of the commodity being smuggled, some of them might find it in their interest to disrupt passage, perhaps to collect the bounteous reward money that would probably be offered by alarmed governments once the uranium theft had been discovered. Once outside the country with their precious booty, terrorists would need to set up a large and well-equipped machine shop to manufacture a bomb and then to populate it with a very select team of highly skilled scientists, technicians, machinists, and administrators. The group would have to be assembled and retained for the monumental task while no consequential suspicions were generated among friends, family, and police about their curious and sudden absence from normal pursuits back home. Members of the bomb-building team would also have to be utterly devoted to the cause, of course, and they would have to be willing to put their lives and certainly their careers at high risk, because after their bomb was discovered or exploded they would probably become the targets of an intense worldwide dragnet operation. Some observers have insisted that it would be easy for terrorists to assemble a crude bomb if they could get enough fissile material. But Christoph Wirz and Emmanuel Egger, two senior physicists in charge of nuclear issues at Switzerland's Spiez Laboratory, bluntly conclude that the task "could hardly be accomplished by a subnational group." They point out that precise blueprints are required, not just sketches and general ideas, and that even with a good blueprint the terrorist group would most certainly be forced to redesign. They also stress that the work is difficult, dangerous, and extremely exacting, and that the technical requirements in several fields verge on the unfeasible. Stephen Younger, former director of nuclear weapons research at Los Alamos Laboratories, has made a similar argument, pointing out that uranium is "exceptionally difficult to machine" whereas "plutonium is one of the most complex metals ever discovered, a material whose basic properties are sensitive to exactly how it is processed." Stressing the "daunting problems associated with material purity, machining, and a host of other issues," Younger concludes, "to think that a terrorist group, working in isolation with an unreliable supply of electricity and little access to tools and supplies" could fabricate a bomb "is farfetched at best." Under the best circumstances, the process of making a bomb could take months or even a year or more, which would, of course, have to be carried out in utter secrecy. In addition, people in the area, including criminals, may observe with increasing curiosity and puzzlement the constant coming and going of technicians unlikely to be locals. If the effort to build a bomb was successful, the finished product, weighing a ton or more, would then have to be transported to and smuggled into the relevant target country where it would have to be received by collaborators who are at once totally dedicated and technically proficient at handling, maintaining, detonating, and perhaps assembling the weapon after it arrives. The financial costs of this extensive and extended operation could easily become monumental. There would be expensive equipment to buy, smuggle, and set up and people to pay or pay off. Some operatives might work for free out of utter dedication to the cause, but the vast conspiracy also requires the subversion of a considerable array of criminals and opportunists, each of whom has every incentive to push the price for cooperation as high as possible. Any criminals competent and capable enough to be effective allies are also likely to be both smart enough to see boundless opportunities for extortion and psychologically equipped by their profession to be willing to exploit them. Those who warn about the likelihood of a terrorist bomb contend that a terrorist group could, if with great difficulty, overcome each obstacle and that doing so in each case is "not impossible." But although it may not be impossible to surmount each individual step, the likelihood that a group could surmount a series of them quickly becomes vanishingly small. Table 1 attempts to catalogue the barriers that must be overcome under the scenario considered most likely to be successful. In contemplating the task before them, would-be atomic terrorists would effectively be required to go though an exercise that looks much like this. If and when they do, they will undoubtedly conclude that their prospects are daunting and accordingly uninspiring or even terminally dispiriting. It is possible to calculate the chances for success. Adopting probability estimates that purposely and heavily bias the case in the terrorists' favor- for example, assuming the terrorists have a 50% chance of overcoming each of the 20 obstacles- the chances that a concerted effort would be successful comes out to be less than one in a million. If one assumes, somewhat more realistically, that their chances at each barrier are one in three, the cumulative odds that they will be able to pull off the deed drop to one in well over three billion. Other routes would-be terrorists might take to acquire a bomb are even more problematic. They are unlikely to be given or sold a bomb by a generous like-minded nuclear state for delivery abroad because the risk would be high, even for a country led by extremists, that the bomb (and its source) would be discovered even before delivery or that it would be exploded in a manner and on a target the donor would not approve, including on the donor itself. Another concern would be that the terrorist group might be infiltrated by foreign intelligence.