A conversation with Allan Friedman about cybersecurity issues

Participants

- Allan Friedman, co-author of *Cybersecurity and Cyberwar: What Everyone Needs to Know*
- Luke Muehlhauser, Executive Director, Machine Intelligence Research Institute (MIRI)

Note: This set of notes was compiled by MIRI and gives an overview of the major points made by Allan Friedman through a combined email and phone interview.

Summary

MIRI spoke with Allan Friedman, co-author of *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Topics include necessary roles of governmental and private entities in the cybersecurity landscape, complexity of necessary legislation, and the role of conventional means and social context in a possible cyberwar or cyber arms race.

Email Interview:

Luke: In *Cybersecurity and Cyberwar: What Everyone Needs to Know*, you and your co-author explain that:

> Today's youth are 'digital natives,' having grown up in a world where computers have always existed and seem a natural feature. But the world is still mostly led by 'digital immigrants,' older generations for whom computers and all the issues the Internet age presents remain unnatural and often confusing.
>
> ...As late as 2001, the Director of the FBI did not have a computer in his office, while the US Secretary of Defense would have his assistant print out e-mails to him, write his response in pen, and then have the assistant type them back in. This sounds outlandish, except that a full decade later the Secretary of Homeland Security, in charge of protecting the nation from cyberthreats, told us at a 2012 conference, 'Don't laugh, but I just don't use e-mail at all.' It wasn't a fear of security, but that she just didn't believe e-mail useful.

As a practical matter, how much do you think it matters that many people in charge of U.S. cybersecurity aren't digital natives? Can the U.S. substantially improve its cybersecurity without many digital natives at the top? Would things change if digital natives were in charge, or are other issues blocking substantive steps toward cybersecurity readiness?

Allan: Comfort with technology is a generational issue, but this doesn't tell the entire story. There are three factors at play, some of which are unique to cybersecurity, and others which are symptomatic of every major evolving political issue.

At the highest level, with members of congress and the judiciary, an unfamiliarity with technology can be quite dangerous. These are people making very important decisions, and if they are dependent on

their aides and clerks to explain things in metaphor, it can lead to misguided and dangerous policy. Young staffers may be digital natives, but that doesn't necessarily mean they are cyber experts. The famous Ted Stevens quote we cite in our book, when the octogenarian Senator explained that the Internet was a "series of tubes," reflects this. You can understand how a staffer tried to explain Internet congestion to him, and he clearly didn't quite get it.

At the same time, much of our national leadership has evolved and learned a great deal. In the Pentagon and in the Executive branch, we've seen a reorientation around how to approach the challenges we face, coming to understand the problem in a more nuanced and detailed fashion. Department of Homeland Security leadership, for example, has grown to both recognize the importance of cybersecurity and the complexities in dealing with the technical and economic issues involved. We've ramped up dozens of new programs and initiatives, led by people who wouldn't count as "digital natives," but definitely appreciate specific challenges, and have the experience needed to drive progress.

The final question is one of the necessary shared expertise required for effective society-wide cyber resilience. How do the pundits talking about tensions in Eastern Europe incorporate cyber risk into their analyses? How do we help middle managers understand cyber risks, and how that relates to their daily jobs? A cyber workforce isn't just the much-needed technical expertise to provide frontline network defenses. It requires integrating a basic understanding of digital risks into everything from the future of smart energy to the evolving relationship between government and the private sector. This may not require true digital natives, but it requires an understanding of what is at stake.

Luke: At another point in the book, you write:

> "As we write, there are some fifty cybersecurity bills under consideration in the US Congress, yet the issue is perceived as too complex to matter in the end to voters, and as a result, the elected representatives who will decide the issues on their behalf. This is one of the reasons that despite all these bills no substantive cybersecurity legislation was passed between 2002 and the writing of this book over a decade later."

Has any "substantive cybersecurity legislation" passed since you wrote the book? What kinds of cybersecurity legislation do you think are most urgently needed at this point?

Allan: The challenge of serious long-term cybersecurity legislation has always been the mismatch in pace between cybersecurity threats and potential legal solutions. It's not just the commonly understood story of ever-present technical innovation, but also the evolving nature of the threat. The risks faced even five years ago are different than those we face today.

In the book, we talk about the need for information sharing, but also explain that it's not a simple problem that a basic law can promote: different types of information sharing pose different benefits and risks.

There are a number of questions in cybersecurity that must be addressed by the government because they are about explicit tradeoffs: how we balance risk. Some of these questions are quite delicate, with very context-dependent details: what are the public and private responsibilities for securing information

infrastructures, or how accountable are publicly traded companies to their shareholders for investing in security and disclosing breaches? These are currently being addressed by various executive agencies, such as the voluntary National Institute of Standards and Technology (NIST) Framework, and the Security and Exchange Commission's voluntary guidelines. If these are found to be insufficient, then congress may have to step in to endow regulatory agencies with more power (in the form of either rewards or punishments) to drive investment and accountability.

Other political questions of balance are about the relative responsibilities of different areas of government. How will we balance the national security community's need to maintain offensive cyber capacity with their mission to defend this country and the rest of the defense establishment's networks and secrets? Do we need regulatory agencies such as the Federal Trade Commission to safeguard consumers?

Finally, the government may have to weigh in private sector questions to help align incentives towards greater security. Are consumer protection laws and state data breach notification laws enough? Who should bear the costs of credit card fraud, and the costs to prevent it? As we learn more about designing better, more secure systems, and as those systems become more integrated into our lives, will we need some sort of liability to encourage better design? These questions can involve picking winners and losers in the private market, and will be very bitterly fought over.

Notes from phone conversation on May 9th:

Inherent tension between technology and risk

Whether dealing with privacy or intellectual property, cybersecurity issues outpace legislation. This is nothing new: innovation happens faster than society and law can catch up. There is an inherent tension between technology and risk. Technological advances have lead to huge gains in productivity, as well as high concentrations of risk through cloud computing, dependence on technical standards, interoperability, and more. It is important for the public to better understand the value of the rewards vs. the risks as they both increase, and to incentivize good security practices. Adam Thierer argues in *Permissionless Innovation* that applying the precautionary principle to technology greatly inhibits innovation: seeking lower risk is a trade-off.

It isn’t possible to expect perfect security, but the public should be able to expect a certain level of security. If a company fails to meet that standard, than a deterrent or punishment may be necessary, to better align the risks between the manufacturers, venders, and users. For example, Google’s Android phone platform is developed by Google, but the operating system is ported to devices by handset manufacturers. In America, the consumer has a relationship with the carrier, who is unable to patch a device, as they neither made the code nor ported it. At present no-one is held accountable for ensuring consumers are protected, and all the risk falls on the consumer.

An expanded role of government in cybersecurity

Monitoring and law enforcement

The Federal Trade Commission has led the way in going after large and small companies that it believes have misled their users in terms of security or privacy. The method of finding and punishing flagrant violators may cause companies to pay attention more quickly than in other, more regulated industries such as energy or health care.

Providing resources and support for ad-hoc, dynamic organizational forums

The legal and economic needs and demands for information sharing are wildly different for different circumstances, and require a flexible approach. For example, if a company is able to detect fraud patterns in users, but it has promised privacy for its users, how does it work with law enforcement? The government needs to support forums that bring together the relevant people with concerns over these issues. This is true for a variety of concerns, from IPv6 conversion or DNS security to the internet governance question.

Promoting and motivating responses to serious cybersecurity issues from the cybersecurity community

There will be incidents where serious expertise on the national security front is critical, but the private sector is likely to supply much of that expertise.

In situations of compromised cybersecurity there are very real trade-offs between mitigating risk, restoring functionality, and gathering intelligence to pursue law enforcement and understand the depth of the threat. The importance of understanding the nature of an attack and innovating a solution to end it may eclipse the importance of incarcerating individual attackers.

How the cyber community deals with new cybersecurity risks

The cybersecurity community often deals with new, unprecedented risks in a serendipitous, decentralized way, without the government playing an explicit role. Affected entities quickly organize, take responsibility, and respond, often with strong financial incentives. For example:

- The recent Heart Bleed bug was a massive interconnected risk, and the established infrastructure organized quickly in response.
- The Conficker bug required software vendors, network vendors and internet software writers to quickly coordinate, address, and shut down the vulnerability.

How should the cyber community deal with new cybersecurity violations?

A very important question is how much we should expect privately held actors to defend what is effectively a public infrastructure. We have learned that when a company reacts quickly and in isolation, this can often shape international policy — for example, when Google reacted to what it considered espionage by withdrawing from China in 2010.

Another approach is ‘hack back,” in which a private actor to respond to attacks without waiting for government process or assistance. Hack back can be seen in two forms:

- A weak form of hack back is to engage in actively gathering threat intelligence. This allows a private entity to better understand the attack and re-think future defenses and reaction.
- A strong form of hack back is to actively 'punish' the attacker, with aggressive, offensive behavior. This is extremely dangerous, and could have unintended consequences.

Importance of conventional warfare issues in the context of cyberwafare

The public often views cyberwar with a focus on the word 'cyber' but ignoring the context of the word 'war'. The United States has a stated policy reserving the right to respond to a cyber-attack with conventional means. Our conventional military complex is more accurate and reliable than our offensive cyber capabilities, so it makes sense to respond to a threat by these means. This may seem dangerous and rash, but a military response to a cyber-attack would be made in the same global context as any other response to an attack on our national defense. Retaliation for cyber-attacks will be incredibly context-dependent and necessitates information on what country is responsible for the attack and why.

A challenge here is the 'attribution problem,' where a government can't decipher the origin of an attack. While this is a real possibility, the attack would have to maintain perfect operational security as well as secure execution, and conventional intelligence gathering would still be an effective tool in compromising operational security.

Special fear of a cyber-attack may in part result from the psychological 'conjunction fallacy', where 'China is likely to launch a cyber-attack', is presumed to be more likely than 'China is likely to launch an attack'.

Important factors in a possible 'cyber arms race'

- It is often assumed with new capabilities that offense is superior to defense. Historically, that is not necessarily true, and may not be true in a future cyber arms race.
- Real people will be the principle vulnerabilities, so conventional intelligence will play a crucial role. Compromising a single individual with proper access would be incredibly valuable and probably much cheaper than a rigorous and tested offensive capacity.
- It Is relatively easy to hack a single computer, but knowing which exact computer to hack is an intelligence question. The cyber arms race will focus on intelligence and counter-intelligence, but now including digital networks, rather than simply human networks.
- Countries' military establishments always compete to have the best technology, but cybersecurity is unique because a third party, the private sector, is independently deciding how to structure and secure itself.

The importance of a public understanding of cybersecurity

Understanding how to reduce cyber risk

Peter W. Singer comments that attacks have happened from picking up a CD or a flash drive from a parking lot or a men's room floor. It is important for the public to understand and advocate for basic, good risk behavior and take cybersecurity seriously.

Correcting fear of technology

More broadly, a basic cybersecurity education will correct against an inflated public fear of the risks of modern technology: the idea that a person could turn off the power grid with a single key stroke, for example. It is important for the public to understand how difficult this would be, and that many proposed solutions to this kind of security threat will not dramatically mitigate that risk without imposing serious and substantial costs.

Cybersecurity is not purely hype, however. It is a real problem that will not fix itself. It is a nuanced task without a single holistic solution, but rather many incremental solutions. The government will have to find its place in the solution, sometimes through new national laws, top-down international efforts, or through governmental agencies and oversight.

All MIRI conversations are available at http://intelligence.org/category/conversations/