Negative Brief: Hack Back

By “Coach Vance” Trefethen

Negative Brief: Hack Back 3

BRIEF NOTES 3

NEGATIVE PHILOSOPHY 3

Exaggerating the “cyber threat” yields negative net benefits. Harms of hype outweigh benefits of improved cyber security 3

Cyber War is just like the Iraq War: Phony inflation of the threat leads to misguided policies 3

SOURCE INDICTMENTS 4

The military and Department of Defense (DoD). They are hyping everything as “cyber” threat to save their budgets 4

Center for Strategic & International Studies, Clarke & Knake, and members of Congress are all exaggerating 4

The Intellectual Property Commission: unqualified and dangerously ignorant 5

IP Commission economic impact numbers are bogus, inflated, and have been debunked over and over. 5

INHERENCY 6

1. Corporate security improvements are solving 6

Increased awareness motivates companies to take more defensive measures now. Golden age of hacking may be over 6

2. US/China negotiations are solving 6

Substantial reduction in Chinese hacking after November 2015 G-20 negotiations 6

HARMS / SIGNIFICANCE 7

1. Hacking threat in general - exaggerated 7

A/T “Chinese hacking threat” – Actually proves China’s weakness, not its strength. 7

Cyber threats of doom are exaggerated: It’s just an excuse for companies to sell more security stuff to the government 7

A/T “Cyber threats are just as dangerous as war or terrorism” –They’re not even close. 7

2. Useless data 8

China has trouble actually doing anything useful with the stolen data 8

They don’t have the skills to do much with stolen technology: too much bureaucracy and not enough technical skills 8

Fears of Chinese cyber threat are exaggerated: Questionable whether they can actually use stolen data 8

Just because they’re stealing tons of data doesn’t mean they know what to do with it 9

China can’t easily absorb the information it gets and probably won’t get any enduring technical advantage 9

They collect cyber industrial espionage data, fine: But then what do they do with it? 9

3. Impacts of hacking are exaggerated 10

A/T “F-35 Joint Strike Force Fighter data stolen in cyber attack” – No impact, no classified info was lost 10

A/T “Defense Dept. computers probed thousands of times/day” – Doesn’t mean any significant problem exists 10

A/T “Power grid blackout ” – Brazil power outage caused by cyber attack turned out to be false 10

Doom scenarios don’t justify action: We survived World War II and Hurricane Katrina, we can survive hacking 11

4. Not much US business impact to IP theft 11

Loss of a trade secret from cyber espionage does not automatically result in economic damage 11

US business impacts of Chinese industrial cyber espionage are exaggerated 11

5. China’s hacking hurts themselves more than it helps 12

Reliance on industrial espionage locks them into permanent “second place” status. Example: Soviets during Cold War 12

6. No Chinese military threat from hacking 12

US/China economic cyber threats will not escalate into a cyber war, nor a conventional war 12

Chinese Army (PLA) would be disadvantaged in a cyber war: The US military is better prepared 12

China’s military cyber capabilities aren’t a big threat 13

China’s cyber capabilities are exaggerated: The gap between them and us is growing (US capabilities are rising faster) 13

SOLVENCY 14

1. Skilled personnel not available for effective hack-back 14

Only a tiny percentage of software professionals have the ability to do hack-back 14

If they didn’t have the skills to prevent the attack, they won’t have the skills to hack back 14

2. Real solvency would require complete NSA control of the internet 14

NSA would have to get into “all the networks” to have a fighting chance of defeating cyber attacks 14

3. Can’t solve for stupidity. 15

Companies know about cyber security risks and don’t take action 15

DISADVANTAGES 15

1. Increased China mistrust 15

Link: Hype about cyber operations raises US/China mistrust 15

Link: Hyping the cyber threat makes US/China war more likely 15

Impact: War with China would be economic and political disaster for both countries 15

2. More hacking in retaliation 16

Link: Hackers may retaliate and increase hacking in response to traps 16

Link & Impact: Retaliation risk and destructive impacts outweigh any possible benefits of hack back. 16

3. Investigation compromised 16

Link: Hack back can harm the investigation of the crime by tainting the evidence 16

Impact: Turn the AFF harms. Now it’s harder to go after the cyber criminals 16

4. Treaty violation 17

Link: The United States signed and ratified a treaty saying we wouldn’t do the Affirmative plan 17

Impact: Lose enforcement of human rights and negative net benefits as the fabric of international law is undermined 17

5. Hype Will Backfire 18

Link: AFF hypes a “threat” with zero casualties. Public will suspect hype is a smokescreen for some other agenda 18

Link: Excess hype will actually reverse public support for cyber security 18

Impact: Turn the harms. Cyber security efforts will crash 18

6. Wasted money 19

Link: Inflating the cyber war threat leads to higher unnecessary federal spending 19

Impact: Every increase in the deficit hurts the economy 19

Works Cited: Hack Back (NEG) 20

Negative Brief: Hack Back

BRIEF NOTES

This is a Negative brief against “THE SOURCE” book case called “Hack Back.” The plan legalizes targets of Chinese computer hackers to “hack back,” that is, take offensive hacking action in response, which is currently illegal. None of the solvency/advocacy evidence says “If we allow hack-back, China will stop (or reduce) hacking.” The biggest solvency barrier is our #1 argument – lack of skilled personnel. After all, if a company or government agency didn’t have the computer skills to prevent someone from hacking their system… how will they have the ability to hack back? We also provide 6 disadvantages, none of which are in THE SOURCE’s negative brief.

This Negative brief contains zero evidence overlap with the NEG brief provided in THE SOURCE, so Affirmatives running this case may not be expecting the material in this brief. It also has evidence against other arguments not made in their plan, in case other versions of this plan are run with different evidence.

NEGATIVE PHILOSOPHY

Exaggerating the “cyber threat” yields negative net benefits. Harms of hype outweigh benefits of improved cyber security

Robert M. Lee & Prof. Thomas Rid 2014. (Lee is an active-duty US Air Force Cyber Warfare Operations Officer who has led multiple cyberspace operations programmes in the Air Force and US Intelligence Community. Rid is a professor in the Department of War Studies at King's College London) Oct 2014 The RUSI JOURNAL Vol 159 Issue 5 “OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy” <http://www.tandfonline.com/doi/full/10.1080/03071847.2014.969932#tabModule>

The Pentagon finds a bit of hype useful to keep the money coming in. The armed services each eye a larger slice of the budget pie. The White House loves some good cyber-angst to nudge law-makers into action. Fear of Chinese cyber-attack makes it easier for members of Congress to relate to voters. Reporting cyber-war means that journalists sell more copy. Academics get quotations and attention from the buzz. Hype up cyber, and everybody wins. However, the real question is whether ramping up the threat of cyberattack is really in everybody's interest. There are downsides to this dynamic. This article argues that cyber is ‘hyped out’. Overstating the threat does not just have benefits (for some): it also comes with significant costs. The benefits are short-lived and easy to spot, whereas the costs are long-term and harder to understand – and they are piling up fast and high. Indeed, they are so high that the debate inches towards a turning point *for all parties involved*.

Cyber War is just like the Iraq War: Phony inflation of the threat leads to misguided policies

Jerry Brito & Tate Watkins 2012. (Brito - was a senior research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program. He also serves as an adjunct professor of law at George Mason University. Watkins - was a research associate for the Technology Policy Program and the State and Local Policy Project.)10 Apr 2012 Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy <http://mercatus.org/sites/default/files/publication/Loving-Cyber-Bomb-Brito-Watkins.pdf>

Different actors— including members of Congress; defense contractors; journalists; policy experts; academics; and civilian, military, and intelligence officials—will each have their own motives for contributing to threat inflation. When a threat is inflated, the marketplace of ideas on which a democracy relies to make sound judgments—in particular, the media and popular debate—can become overwhelmed by fallacious information. The result can be unwarranted public support for misguided policies. The run-up to the Iraq War illustrates the dynamic of threat inflation, and the current conversation around cybersecurity exhibits striking parallels to that period.

SOURCE INDICTMENTS

The military and Department of Defense (DoD). They are hyping everything as “cyber” threat to save their budgets

Robert M. Lee & Prof. Thomas Rid 2014. (Lee is an active-duty US Air Force Cyber Warfare Operations Officer who has led multiple cyberspace operations programmes in the Air Force and US Intelligence Community. Rid is a professor in the Department of War Studies at King's College London) Oct 2014 The RUSI JOURNAL Vol 159 Issue 5 “OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy” <http://www.tandfonline.com/doi/full/10.1080/03071847.2014.969932#tabModule>

The DoD's overall budget is shrinking fast; upwards of 100,000 personnel are expected to be cut as the Pentagon reduces the budget by more than $75 billion over the next two years.Budget cuts and an uncertain fiscal climate have led to the scrapping of programmes, capabilities and even entire agencies. Yet the cyber budget is growing. As revealed by the 2015 annual budget report, cyber-security is one of the few areas receiving more funding, not less – for research, defensive and offensive operations, and acquisition – mostly tied to US Cyber Command and the NSA. This has created a climate in which it is beneficial to have a tie-in to cyber. Programme managers know that if a budget could land on the chopping board, relabelling it as – or intertwining it with – ‘cyber-something’ could save it. Everybody uses computers, after all, and everybody wants them to be safe.

Center for Strategic & International Studies, Clarke & Knake, and members of Congress are all exaggerating

Jerry Brito & Tate Watkins 2011. (Brito - was a senior research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program. He also serves as an adjunct professor of law at George Mason University. Watkins - was a research associate for the Technology Policy Program and the State and Local Policy Project.) 26 Apr 2011 Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy <http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy-0> (brackets added)

The potential for cyber threat inflation remains high. Countless legislators and executive branch officials have called for increased federal involvement in cybersecurity, citing cyber-doom scenarios as their rationale. But they have not presented verifiable evidence of the existential threats they warn about. The influential CSIS [Center for Strategic & International Studies] Commission Report conflates cyber threats and asserts without evidence that wide-reaching federal cybersecurity legislation is imperative. Clarke and Knake make similar assertions in Cyber War, but also fail to differentiate the disparate cyber threats or offer evidence to bolster their claims of cyber catastrophe. Credulous reporting by major media outlets that often cite only anonymous sources further inflates threats, even though many of these stories are hyperbolic or later debunked. Still, members of Congress have cited such accounts in proposing legislation, often warning of potential cyber catastrophes but rarely presenting verifiable evidence of catastrophic threats. Before the federal government’s role in cybersecurity policy can be determined, doomsayers must present verifiable evidence of the types of threats they warn about to the public.

The Intellectual Property Commission: unqualified and dangerously ignorant

Lauren Weinstein 2013 (worked in the early 1970s at the first site on the ARPANET, the origin of the internet, which was located at UCLA. He was the co-founder of People For Internet Responsibility (PFIR) and the co-founder of the Union for Representative International Internet Cooperation and Analysis; has been a columnist for Wired News and a commentator on National Public Radio) 24 May 2013 “USA Intellectual Property Theft Commission Recommends Malware!” <http://lauren.vortex.com/archive/001034.html> (brackets added)

And what they're proposing is no less than the legitimizing of a form of malware that has attacked vast numbers of Internet users, costing them immense lost time, money, and grief. You may have been unlucky enough to see this for yourself. It comes in various forms, but generally it claims to be a law enforcement warning (often saying it's from the FBI). It accuses you of having some kind of "illicit" material (usually a copyright violation and/or porn) on your system, and demands that you contact an address for "more information" -- or even that you make immediate payment of a "fine" to release your computer. Your webcam may even be surreptitiously used to include your photo to further confuse and upset you. Of course, this is all a scam. If you go to that address, you'll likely download more malware, or be directed to provide credit card or bank account info to pay for your "violation" of law. Even if you pay, you have no assurance that this malware will go away. Even if it does seem to release you, it may hang around in the background sucking up your private information, bank account access data, and who knows what else. Consumers attacked by this class of malware have spent enormous sums to get it actually cleaned out, and very many have been directly defrauded by it as well. And of course, these systems can't be used for anything else while the malware is actively threatening you. So now we have the IP Commission suggesting that firms be allowed to use basically this same technique -- pop up on someone's computer because you \*believe\* they've stolen something from you, terrify them with law enforcement threats, and lock them out of their (possibly crucial) data and applications as well. What the [expletive deleted] are these guys thinking? Outside of the enormous collateral damage this sort of "permitted malware" regime could do to innocents -- how would the average user be able to tell the difference between this class of malware and the fraudulent variety that is currently a scourge across the Net? What's more, how can it possibly be justified to lock users out of their systems on this sort of unilateral basis? How much "theft" -- even when it actually occurred -- is enough to justify locking someone out of their private applications and data, some of which may be absolutely necessary to their daily lives. I could get into a lot of technical details about this, but we can just cut to the chase for now: the whole concept is utterly insane, and frankly calls into question the competency of the commission in general. With our own commissions coming up with idiotic, dangerous nonsense like this, we may have more to worry about from their kind of thinking than from the "cyber-crooks" themselves.

IP Commission economic impact numbers are bogus, inflated, and have been debunked over and over.

Mike Masnick 2013 (bachelor's degree in Industrial and Labor Relations and an MBA from Cornell University; CEO and founder of Techdirt, a weblog that focuses on technology news and tech-related issues; founder and CEO of the company Floor64 and a contributor at BusinessWeek) 28 MAY 2013 Fear Mongering Report Suggests 'IP Theft From China' One Of The Biggest Problems America Faces <https://www.techdirt.com/articles/20130526/22281723217/fear-mongering-report-suggests-ip-theft-china-one-biggest-problems-america-faces.shtml> (parentheses and ellipses in original)

Even worse, it completely ignores the fact that the $200 billion estimate it extrapolates as one basis for claiming $300 billion has been [debunked](https://www.techdirt.com/articles/20100801/17431810439.shtml) over and over again, and is based on layers upon layers of bogus premises from decades ago, that today is just expanded every few years by lobbyists who insist it's growing. Of course, when the actual numbers were looked at closely, it was discovered that a more accurate assessment might be about 2% of that number. But Huntsman and Blair instead insist that the $300 billion is probably too low. Based on what? Nothing. Just the fear mongering they hear from companies and lobbyists -- the same companies who certainly have a very strong vested interest in protectionism against Chinese competitors (oh wait...).

INHERENCY

1. Corporate security improvements are solving

Increased awareness motivates companies to take more defensive measures now. Golden age of hacking may be over

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

Prior to 2010, Western firms could be accused of complacency regarding cybersecurity. Since then, however, Western cybersecurity defenses, technical expertise, and government assistance to firms have improved. Also, the increased reporting on long-duration APTs (i.e., those that might be expected to be the most difficult to root out) may reflect a growing discovery rate of hard-to-find APTs by network defenders. The potential improvement in Western cyber defense stands in stark contrast to the popular perception of helplessness in the face of growing Chinese intrusion threats. It is possible that one day Chinese cyber operators may look back on 2010–13 much the way German submariners looked back on the “happy time” of 1940–41—namely, as a brief period rich in easy targets before victims learned how to develop active tracking and countermeasures to protect themselves.

1. US/China negotiations are solving

Substantial reduction in Chinese hacking after November 2015 G-20 negotiations

Emilio Iasiello 2015 (cyber threat analyst for the past thirteen years working as a government contractor and a government civilian in the Department of State as well as the Department of Defense, as well as as well as private sector companies ) “Ramping Down Chinese Commercial Cyber Espionage” FOREIGN POLICY JOURNAL 9 Dec 2015 <http://www.foreignpolicyjournal.com/2015/12/09/ramping-down-chinese-cyber-espionage/>

Despite criticism from skeptics, China is trying to honor its “no commercial hacking for profit” commitments as first promised in an accord with the United States, and later reaffirmed at the November 2015 G20 summit. Recent news reports cited that in a show of good faith, China had arrested hackers per the U.S. government’s request prior to meeting with President Obama in September. While detractors believe that commercial cyber espionage hasn’t really stopped, recent Chinese efforts show a government trying to get a handle on its large spying apparatus that could include hired and independent contractors acting autonomously in addition to its other resources. While complete cessation may never occur, significant timely reduction demonstrates Beijing’s willingness to work with the United States as a partner and not a pariah, and provides a foundation from which the two governments can move forward on other cyber security areas where incongruity persists.

HARMS / SIGNIFICANCE

1. Hacking threat in general - exaggerated

A/T “Chinese hacking threat” – Actually proves China’s weakness, not its strength.

Robert M. Lee & Prof. Thomas Rid 2014. (Lee is an active-duty US Air Force Cyber Warfare Operations Officer who has led multiple cyberspace operations programmes in the Air Force and US Intelligence Community. Rid is a professor in the Department of War Studies at King's College London) Oct 2014 The RUSI JOURNAL Vol 159 Issue 5 “OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy” <http://www.tandfonline.com/doi/full/10.1080/03071847.2014.969932#tabModule>

The Department of Justice could have pointed out what a solid and hype-repellent intelligence analysis would surely bring to light – that what looks like state-controlled Chinese cyber-espionage from the vantage point of the Western District of Pennsylvania looks rather different from Beijing: it looks like a lack of state control and deeply entrenched corruption. It is highly likely that various PLA units receive some of their tasking not only from their civilian leaders in the Communist Party, but also through shady backchannels and personal connections directly from state-owned enterprises that are taking advantage of idle PLA resources. The kind of targeting and tasking that the indictment revealed is probably too precise to be requested by senior government officials. Pointing this out would have been more embarrassing for Beijing – as well as being more difficult for it to counter – and diplomatically less damaging. Lower the pitch, and 61398 is code for China's weakness rather than its strength.

Cyber threats of doom are exaggerated: It’s just an excuse for companies to sell more security stuff to the government

Jerry Brito & Tate Watkins 2011. (Brito - was a senior research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program. He also serves as an adjunct professor of law at George Mason University. Watkins - was a research associate for the Technology Policy Program and the State and Local Policy Project.) 26 Apr 2011 Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy <http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy-0>

Security risks to private and government networks from criminals and malicious state actors are no doubt real and pressing. However, the rhetoric of “cyber doom” employed by proponents of increased federal intervention in cybersecurity implies an almost existential threat that requires instant and immense action. Yet these proponents lack clear evidence of such doomsday threats that can be verified by the public. As a result, the United States may be witnessing a bout of threat inflation similar to that seen in the run-up to the Iraq War. Additionally, a cyber-industrial complex is emerging, much like the military-industrial complex of the Cold War. This complex may serve not only to supply cybersecurity solutions to the federal government, but to drum up demand for those solutions as well.

A/T “Cyber threats are just as dangerous as war or terrorism” –They’re not even close.

Micah Zenko 2014. (the Douglas Dillon Fellow with the Center for Preventive Action at the Council on Foreign Relations) FOREIGN POLICY, “Exaggeration Nation” 21 Nov 2014 <http://foreignpolicy.com/2014/11/21/exaggeration-nation/?wp_login_redirect=0> (Brackets added; ellipses in original)

Furthermore, to more consistently represent his views, [Defense Secretary] Hagel has likewise portrayed the threats from other sources inaccurately, [stating](http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5485) that "cyber threats, which are relatively new … are just as real and deadly and lethal as anything we’ve ever dealt with." (Last year, an estimated 37,992 people died in armed conflicts, and zero from cyberattacks.)

2. Useless data

China has trouble actually doing anything useful with the stolen data

Dr Jon R. Lindsay 2015 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) May 2015 **"Exaggerating the Chinese Cyber Threat"** <http://belfercenter.ksg.harvard.edu/publication/25321/exaggerating_the_chinese_cyber_threat.html>

There is strong evidence that China continues to engage in aggressive cyber espionage campaigns against Western interests. Yet it struggles to convert even legitimately obtained foreign data into competitive advantage, let alone make sense of petabytes of stolen data. Absorption is especially challenging at the most sophisticated end of the value chain (e.g., advanced fighter aircraft), which is dominated by the United States. At the same time, the United States conducts its own cyber espionage against China , as the Edward Snowden leaks dramatized, which can indirectly aid U.S. firms (e.g., in government trade negotiations). China's uneven industrial development, fragmented cyber defenses, erratic cyber tradecraft, and the market dominance of U.S. technology firms provide considerable advantages to the United States.

They don’t have the skills to do much with stolen technology: too much bureaucracy and not enough technical skills

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

China faces major challenges in converting foreign inputs into innovative output given the notoriously compartmentalized and hierarchical nature of Chinese bureaucracy, underdeveloped high-end equipment manufacturing capacity, and chronic dependence on foreign technology and know-how. Reliance on Russia for fighter jet engines despite years of access to technical design information and assistance from Russian technicians is a particularly notable but hardly unique example in the Chinese defense industry. Foreign expertise is only one input in the overall innovation process, which also requires “hard” factors such as materials, universities, skilled labor, laboratories, and factories, as well as “soft” factors such as leadership, regulation, contract enforcement, standards and protocols, and an innovative culture. The utility of even the best CNE [computer network exploitation] is sensitive to the performance of the rest of these factors working in synergy, and China still has far to go in integrating them.

Fears of Chinese cyber threat are exaggerated: Questionable whether they can actually use stolen data

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://muse.jhu.edu/login?auth=0&type=summary&url=/journals/international_security/v039/39.3.lindsay.pdf>

Exaggerated fears about the paralysis of digital infrastructure and the loss of competitive advantage contribute to a spiral of mistrust in U.S.-China relations. In every category of putative Chinese cyber threat, there are also considerable Chinese vulnerabilities and Western advantages. China has inadvertently degraded the economic efficiency of its networks and exposed them to foreign infiltration by prioritizing political information control over technical cyber defense. Although China also actively infiltrates foreign targets, its ability to absorb stolen data is questionable, especially at the most competitive end of the value chain, where the United States dominates.

Just because they’re stealing tons of data doesn’t mean they know what to do with it

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf> (brackets added)

Remote access to target networks is only the first step toward developing an intelligence advantage, much less downstream competitive advantage. Although Western cyber defenders can observe the exfiltration of petabytes of data to Chinese servers, they cannot so readily measure China’s ability to use the data. It is possible, for example, that operators in the Third Department of the PLA General Staff are simply rewarded for the number of foreign targets penetrated and terabytes exfiltrated, with little attention to the satisfaction of the intelligence customer, thereby creating lots of measurable CNE [computer network exploitation] with little improvement in national competitiveness. The acquisition, absorption, and application of foreign information from any source is a complicated process. Transaction costs at every step along the way caused by information overload, analytic misinterpretation, or bureaucratic silos can undermine the translation of stolen data into new production knowledge and successful competition in the marketplace.

China can’t easily absorb the information it gets and probably won’t get any enduring technical advantage

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

Chinese espionage is impressive in its scope, but it does not translate easily into industrial absorption, which is a prerequisite for competitive advantage. Furthermore, U.S. intelligence appears to be more technically adept, even if its target set differs somewhat from China’s. Both sides are engaged in commercial and intelligence contests using a range of political, economic, and technical tools. Charges of unfair competition and attempts to redress it will remain a chronic feature of U.S.-China relations. There is no reason to expect the side playing catch-up to realize an enduring advantage for technical reasons alone.

They collect cyber industrial espionage data, fine: But then what do they do with it?

*Greg Austin 2013. (Professorial Fellow with the* [East-West Institute](http://thediplomat.com/2015/05/what-the-us-gets-wrong-about-chinese-cyberespionage/www.ewi.info) *in New York and a Visiting Professor at the Australian Centre for Cyber Security in the University of New South Wales at the Australian Defense Force Academy) 26 Sept 2013* China’s Cyber Espionage Priorities <http://ewipolicy.tumblr.com/post/62325267109/chinas-cyber-espionage-priorities>

As we contemplate the international threat picture for cybersecurity, how can we evaluate claims about China’s cyber espionage intended to aid Chinese firms in production of items copied from competitors’ designs? According to some sources, the country is engaged in the biggest illicit transfer of wealth in history through the theft of intellectual property from the United States and other advanced economies. The United States has, according to newspaper reports, compiled several case studies demonstrating specific IP theft by Chinese government actors that has been converted to competitor production and that undercut the original American IP owner’s profitability. Beyond these few cases, one of the gaps in the publicly available allegations is a fine-grained and comprehensive analysis of how exactly Chinese intelligence agencies handle the information they are allegedly vacuuming up by the terabyte. Do they have an army of technically skilled translators who immediately render all documents into Chinese? Or is there an intermediary team of technically qualified staff brought in from China’s R&D establishments, specific to each design secret being reviewed, to make a judgment that a particular document needs to be translated and then to determine who in the industry should receive it to set about copying it? In the absence of any discussion in public by United States official sources of this sort of fine-grained detail, we are left to make our own thinly-sourced assessment.

3. Impacts of hacking are exaggerated

A/T “F-35 Joint Strike Force Fighter data stolen in cyber attack” – No impact, no classified info was lost

Jerry Brito & Tate Watkins 2011. (Brito - was a senior research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program. He also serves as an adjunct professor of law at George Mason University. Watkins - was a research associate for the Technology Policy Program and the State and Local Policy Project.) 26 Apr 2011 Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy <http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy-0>

The author of the article, Siobhan Gorman, also contributed to another front-page Wall Street Journal cybersecurity scoop reporting that spies had infiltrated Pentagon computers and had stolen terabytes of data related to the F-35 Joint Strike Fighter. The only sources for that report were “current and former government officials familiar with the attacks.” Later reporting by the Associated Press, also citing anonymous officials, found that no classified information was compromised in the breach. Unfortunately, without any official statement on the matter, the result of these reports can well be to raise public alarm without offering a clear sense of the scope or magnitude of the threat.

A/T “Defense Dept. computers probed thousands of times/day” – Doesn’t mean any significant problem exists

Jerry Brito & Tate Watkins 2011. (Brito - was a senior research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program. He also serves as an adjunct professor of law at George Mason University. Watkins - was a research associate for the Technology Policy Program and the State and Local Policy Project.)26 Apr 2011 Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy <http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy-0>

The report notes that Department of Defense computers are “probed hundreds of thousands of times each day.” This is a fact that proponents of increased federal involvement in cybersecurity often cite as evidence for a looming threat. However, probing and scanning networks are the digital equivalent of trying doorknobs to see if they are unlocked—a maneuver available to even the most unsophisticated would-be hackers. The number of times a computer network is probed is not evidence of an attack, a breach, or even of a problem.

A/T “Power grid blackout ” – Brazil power outage caused by cyber attack turned out to be false

Jerry Brito & Tate Watkins 2011. (Brito - was a senior research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program. He also serves as an adjunct professor of law at George Mason University. Watkins - was a research associate for the Technology Policy Program and the State and Local Policy Project.) 26 Apr 2011 Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy <http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy-0>

That front page Wall Street Journal article from April 2009 is often cited as evidence for the proposition that the power grid is rigged to blow, but it could just as easily be cited as an example of “mere conduit” reporting. Similar to Judith Miller’s Iraq WMD articles, the only sources for the article’s claim that key infrastructure has been compromised are anonymous U.S. intelligence officials. With little specificity about the alleged infiltrations, readers—whether academics, journalists, or the lay public—are left with no way to verify the claims. The article does cite a public pronouncement by senior CIA official Tom Donahue that a cyber attack had caused multiple power outages overseas. But Donahue’s pronouncement is what Clarke and Knake cite for their claim that cyber attacks caused a blackout in Brazil, which we now know is untrue.

Doom scenarios don’t justify action: We survived World War II and Hurricane Katrina, we can survive hacking

Jerry Brito & Tate Watkins 2011. (Brito - was a senior research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program. He also serves as an adjunct professor of law at George Mason University. Watkins - was a research associate for the Technology Policy Program and the State and Local Policy Project.) 26 Apr 2011 Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy <http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy-0> (Brackets in original)

Finally, it should be pointed out that even if one were to determine that cybersecurity is under-provided by the private sector, one would then have to proceed to the next questions in an economic analysis: consider different alternatives to regulation, as well as alternative forms of regulation, and determine whether the benefits of the chosen alternative outweigh its costs. Indeed, although cyber-doom scenarios are often presented as existential threats to our fragile interconnected society, the evidence from history—from WWII to 9/11 to Katrina—is that people and institutions are incredibly resilient and would likely bounce back from any probable cyber attack. As Aaron Wildavsky puts it when addressing how best to respond to dangers that cannot be understood in advance: “[m]y vote goes to the resilience that comes from passing many trials and learning from errors so that the defects of society’s limited imagination are made up by larger amounts of global resources that can be converted into meeting the dangers that its members never thought would arise.”

4. Not much US business impact to IP theft

Loss of a trade secret from cyber espionage does not automatically result in economic damage

*Greg Austin 2015. (Professorial Fellow with the* [East-West Institute](http://thediplomat.com/2015/05/what-the-us-gets-wrong-about-chinese-cyberespionage/www.ewi.info) *in New York and a Visiting Professor at the Australian Centre for Cyber Security in the University of New South Wales at the Australian Defense Force Academy)* China’s Cyberespionage: The National Security Distinction and U.S. Diplomacy, May 2015 <http://thediplomat.com/wp-content/uploads/2015/05/thediplomat_2015-05-21_22-14-05.pdf>

In the indictments, the United States says it has evidence of transfer of trade secrets to civil sector companies in the cases of Westinghouse and USS, but while other instances have been asserted, few have been evidenced. It is axiomatic that loss of a trade secret does not automatically convert to damaging competition any more than theft of credit card details translates into losses for all of the victims. In fact, very few people suffer personal financial losses as result of the theft and illegal sale of millions of credit card details.

US business impacts of Chinese industrial cyber espionage are exaggerated

Dr Jon R. Lindsay 2015 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) May 2015 **"Exaggerating the Chinese Cyber Threat"** <http://belfercenter.ksg.harvard.edu/publication/25321/exaggerating_the_chinese_cyber_threat.html>

The rhetorical spiral of mistrust in the Sino-American relationship threatens to undermine the mutual benefits of the information revolution. Fears about the paralysis of the United States' digital infrastructure or the hemorrhage of its competitive advantage are exaggerated. Chinese cyber operators face underappreciated organizational challenges, including information overload and bureaucratic compartmentalization, which hinder the weaponization of cyberspace or absorption of stolen intellectual property. More important, both the United States and China have strong incentives to moderate the intensity of their cyber exploitation to preserve profitable interconnections and avoid costly punishment. The policy backlash against U.S. firms and liberal internet governance by China and others is ultimately more worrisome for U.S. competitiveness than espionage; ironically, it is also counterproductive for Chinese growth. The United States is unlikely to experience either a so-called digital Pearl Harbor through cyber warfare or death by a thousand cuts through industrial espionage.

5. China’s hacking hurts themselves more than it helps

Reliance on industrial espionage locks them into permanent “second place” status. Example: Soviets during Cold War

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf> (brackets added)

The Soviet Union’s reliance on systematic industrial espionage to catch up with the West provides a cautionary tale: the Soviet system became optimized for imitation rather than innovation and was thus locked into a form of second-place dependency, even as it shortened research and development timelines. Chinese espionage can potentially narrow the gap with the West, but only at the price of creating dependency through investment in a large-scale absorption effort. Chinese CNE [computer network exploitation] poses a genuine intelligence threat, to be sure, but it is neither singularly grave nor unprecedented.

6. No Chinese military threat from hacking

US/China economic cyber threats will not escalate into a cyber war, nor a conventional war

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

This article argues that for every type of purported Chinese cyber threat, there are also serious Chinese vulnerabilities and Western strengths that reinforce the political status quo. Cyberwar between the United States and China, much like U.S.-China conventional war, is highly unlikely. Nevertheless, the economically driven proliferation of information technology enables numerous instances of friction to emerge below the threshold of violence.

Chinese Army (PLA) would be disadvantaged in a cyber war: The US military is better prepared

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

If cyberwarfare is as effective as Chinese writers believe it is but they underestimate the costs of mastery, then the PLA is doubly disadvantaged. Chinese attacks can be expected to be less skillfully coordinated against more robust U.S. defenses, and vice versa. The United States already has, while China still struggles to develop, the institutional complements and experience required to plan and control cyber operations in synchrony with the larger battle. Meanwhile the fear of cyberwarfare has prompted considerable U.S. military investment in network protection, active cyber defense measures (e.g., counterintelligence deception and “hack back” counterattack), and exercises in cyber-degraded conditions. The vaunted asymmetry of cyberwarfare, usually posed as an advantage for the weaker power, in fact runs in the opposite direction, giving the stronger and more experienced force the advantage.

China’s military cyber capabilities aren’t a big threat

Dr Jon R. Lindsay 2015 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) May 2015 **"Exaggerating the Chinese Cyber Threat"** <http://belfercenter.ksg.harvard.edu/publication/25321/exaggerating_the_chinese_cyber_threat.html>

Despite high levels of Chinese political harassment and espionage, there is little evidence of skill or subtlety in China's military cyber operations. Although Chinese strategists describe cyberspace as a highly asymmetric and decisive domain of warfare, China's military cyber capacity does not live up to its doctrinal aspirations. A disruptive attack on physical infrastructure requires careful testing, painstaking planning, and sophisticated intelligence. Even experienced U.S. cyber operators struggle with these challenges. By contrast, the Chinese military is rigidly hierarchical and has no wartime experience with complex information systems. Further, China's pursuit of military "informatization" (i.e., emulation of the U.S. network-centric style of operations) increases its dependence on vulnerable networks and exposure to foreign cyberattack. To be sure, China engages in aggressive cyber campaigns, especially against nongovernmental organizations and firms less equipped to defend themselves than government entities. These activities, however, do not constitute major military threats against the United States, and they do nothing to defend China from the considerable intelligence and military advantages of the United States.

China’s cyber capabilities are exaggerated: The gap between them and us is growing (US capabilities are rising faster)

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction http://belfercenter.ksg.harvard.edu/files/IS3903\_pp007-047.pdf

Although China also actively infiltrates Western networks, its ability to absorb stolen data is questionable, especially at the most competitive end of the value chain, where the United States dominates. Similarly, China’s military cyber capacity cannot live up to its aggressive doctrinal aspirations, even as “informatization” creates vulnerabilities that more experienced foreign cyber operators can attack. Outmatched by the West, China has resorted to a strategy of institutional reform, but it benefits too much from multistakeholder governance to pose a credible alternative. The secrecy of cyber capabilities and operations on all sides makes it difficult to estimate with confidence the magnitude of the gap between China and the United States in the balance of cyber power, but it is potentially growing, not shrinking.

SOLVENCY

1. Skilled personnel not available for effective hack-back

Only a tiny percentage of software professionals have the ability to do hack-back

Lance Deviney 2014 (career intelligence officer specializing in advanced intelligence, surveillance, reconnaissance, signal exploitation, and cyber security; Bachelor’s degree in Computer Studies from the U. of Maryland University College, Master of Arts degree in National Security Studies with an emphasis on Terrorism from American Military Univ. and a Master of Professional Studies degree from Penn. State Univ. in Homeland Security with a focus on Information Security & Forensics.;holds graduate-level certificates in Telecommunications Technology from George Washington Univ and Information Systems Security from the Penn State Univ.) TOP CYBER: DEVELOPING THE TOP ONE PERCENT TO DEFEAT THE ADVANCED PERSISTENT THREAT 13 Feb 2014 <http://www.au.af.mil/au/awc/awcgate/awc/2014_deviney.pdf>

In the commercial world, the majority of computer security professionals are in the business of providing services and defending them: ensuring network integrity, operating intrusion detection systems, installing vulnerability patches, and keeping core services at a high state of availability. A much smaller subset performs network oversight, reconnaissance, sleuthing, and penetration testing and hunting for hidden intruders in their networks. An even tinier percentage, comprising the highest educated, trained and proficient SMEs have the prowess and accompanying authority to conduct advanced, and arguably dangerous actions, such as hacking back into an intruder’s host machine to disable their system through active defensive means.

If they didn’t have the skills to prevent the attack, they won’t have the skills to hack back

Jody Westby 2012 (CEO of Global Cyber Risk and provide consulting services in the areas of privacy, security, cybercrime, and IT governance; Adjunct Professor at Georgia Institute of Technology's School of Computer Science; Distinguished Fellow for Carnegie Mellon CyLab; chair of the American Bar Association’s Privacy & Computer Crime Committee ) FORBES magazine 29 Nov 2012 “Caution: Active Response to Cyber Attacks Has High Risk” <http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/#335808882cd0> (brackets added)

“If a company does not have the skills to defend its systems, it likely does not have the skills to attack back — or make decisions about whether to engage in such actions. Hiring a third party to attack in an offensive role is risky, since most corporate executives are naive about the complexity of the cyber criminal’s tool sets,” he [Research Scientist and Engineer Principal at the [Univ. of Washington](http://www.forbes.com/colleges/university-of-washington-seattle-campus/)‘s Applied Physics Laboratory, Dave Dittrich] added.

1. Real solvency would require complete NSA control of the internet

NSA would have to get into “all the networks” to have a fighting chance of defeating cyber attacks

Prof. Jack Goldsmith 2013 (Professor at Harvard Law School, where he teaches and writes about national security law, presidential power, cybersecurity, international law, internet law, foreign relations law, and conflict of laws; former Assistant Attorney General, Office of Legal Counsel ) 10 Oct 2013 “We Need an Invasive NSA” THE NEW REPUBLIC <http://www.newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks> (brackets added)

The U.S. government can fully monitor air, space, and sea for potential attacks from abroad. But it has limited access to the channels of cyber-attack and cyber-theft, because they are owned by private telecommunication firms, and because Congress strictly limits government access to private communications. “I can’t defend the country until I’m into all the networks,” [NSA Director] General Alexander reportedly told senior government officials a few months ago. For Alexander, being in the network means having government computers scan the content and metadata of Internet communications in the United States and store some of these communications for extended periods. Such access, he thinks, will give the government a fighting chance to find the needle of known malware in the haystack of communications so that it can block or degrade the attack or exploitation.

3. Can’t solve for stupidity.

Companies know about cyber security risks and don’t take action

Michael Riley and Ben Elgin 2013 (journalists) BLOOMBERG NEWS 2 May 2013 “China’s Cyberspies Outwit Model for Bond’s Q” <http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html>

The hackers logged on through the company’s remote access system, just like any employee. It was a trick they were able to use only because QinetiQ didn’t employ two-factor authentication, a simple device that generates a unique code employees enter, along with their usual password, anytime they work from home. The problem had been spotted months earlier in a security review. Mandiant, which worked on several TSG breaches and performed the test, recommended a relatively inexpensive fix. The advice was ignored, according to a person familiar with the report.

DISADVANTAGES

1. Increased China mistrust

Link: Hype about cyber operations raises US/China mistrust

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

Cyber operations and the rhetorical reactions to them on both sides of the Pacific have undermined trust in the Sino-American relationship. Exaggerated fears about the paralysis of digital infrastructure and growing concerns over competitive advantage exacerbate the spiral of mistrust. Closer consideration of domestic factors within China and China’s strategic interaction with the United States reveals a more complicated yet less worrisome situation.

Link: Hyping the cyber threat makes US/China war more likely

Dr Jon R. Lindsay 2014 ( PhD in Political Science from M.I.T.; Assistant Research Scientist at Univ of California Institute on Global Conflict and Cooperation) The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>

As long as dense interconnection and economic interdependence remain mutually beneficial for powers such as the United States and China, they will be able to tolerate the irritants that they will inevitably inflict on one another. The modern intelligence-counterintelligence contest plays out in a complicated sociotechnical space where states take advantage of economic cooperation and hedge against security competition. If their broader mutual interest frays, however, then cyberwarfare becomes just one facet of a more serious strategic problem involving more dangerous means. Exaggeration of the cyber threat feeds spirals of mistrust, which make this undesirable outcome slightly more likely.

Impact: War with China would be economic and political disaster for both countries

Dr. Ted Galen Carpenter 2004 ( PhD in Diplomatic History; vice president for defense and foreign policy studies at the Cato Institute, is the author of eight books on international issues) 10 Aug 2004, "China's Taiwan Policy and America's Difficult Choices" <http://www.cato.org/pub_display.php?pub_id=2778>

And a war in the Taiwan strait would be a disaster for both the PRC and the United States. The mutually beneficial economic relationship (now valued at more than $150 billion a year) would be severed, and America's relations with a major power would be poisoned for decades.

2. More hacking in retaliation

Link: Hackers may retaliate and increase hacking in response to traps

Loras R. Evans 2000. (managing director with the technology risk advisory services group in RSM McGladrey, Inc.) Intrusion Detection FAQ: What is a Honeypot? <https://www.sans.org/security-resources/idfaq/honeypot3.php>

The second main caveat for consideration is whether hacking organizations will rally against an organization that has set "traps" and make them a public target for other hackers. Examples of this sort of activity can be found easily on any of the popular hacker’s sites or their publications.

Link & Impact: Retaliation risk and destructive impacts outweigh any possible benefits of hack back.

Jody Westby 2012 (CEO of Global Cyber Risk and provide consulting services in the areas of privacy, security, cybercrime, and IT governance; Adjunct Professor at Georgia Institute of Technology's School of Computer Science; Distinguished Fellow for Carnegie Mellon CyLab; chair of the American Bar Association’s Privacy & Computer Crime Committee ) FORBES magazine 29 Nov 2012 “Caution: Active Response to Cyber Attacks Has High Risk” <http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/#335808882cd0>

The perceived value of active defense has to be weighed against the risk and cost. On the risk side, there is the clear possibility that playing cat and mouse with sophisticated cybercriminals may cause them to up the stakes and launch more destructive attacks…even after lying low for a considerable period of time. John Pescatore, head of [Gartner](http://blogs.forbes.com/gartnergroup/)‘s Internet security practice, was quoted in a [Reuters article](http://www.reuters.com/article/2012/06/17/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120617) as saying, “There is no business case for it and no possible positive outcome.”

1. Investigation compromised

Link: Hack back can harm the investigation of the crime by tainting the evidence

Jody Westby 2012 (CEO of Global Cyber Risk and provide consulting services in the areas of privacy, security, cybercrime, and IT governance; Adjunct Professor at Georgia Institute of Technology's School of Computer Science; Distinguished Fellow for Carnegie Mellon CyLab; chair of the American Bar Association’s Privacy & Computer Crime Committee ) FORBES magazine 29 Nov 2012 “Caution: Active Response to Cyber Attacks Has High Risk” <http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/#335808882cd0> (brackets added)

Another consideration is that active defense may taint the evidence needed for an investigation. “If victims want to engage in aggressive investigative activities, they need to also acknowledge the potential harm that they may be inflicting to the investigative process and other systems,” observes [Research Scientist and Engineer Principal at the [Univ. of Washington](http://www.forbes.com/colleges/university-of-washington-seattle-campus/)‘s Applied Physics Laboratory, Dave] Dittrich.

Impact: Turn the AFF harms. Now it’s harder to go after the cyber criminals

4. Treaty violation

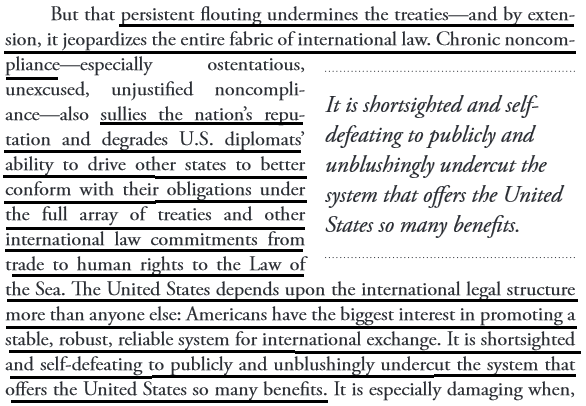
Link: The United States signed and ratified a treaty saying we wouldn’t do the Affirmative plan

Jody Westby 2012 (CEO of Global Cyber Risk and provide consulting services in the areas of privacy, security, cybercrime, and IT governance; Adjunct Professor at Georgia Institute of Technology's School of Computer Science; Distinguished Fellow for Carnegie Mellon CyLab; chair of the American Bar Association’s Privacy & Computer Crime Committee ) FORBES magazine 29 Nov 2012 “Caution: Active Response to Cyber Attacks Has High Risk” <http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/#335808882cd0>

 If U.S. companies start hacking back into systems in other countries, a diplomatic crisis is sure to follow. Foreign governments will rightly complain to the U.S. and may even accuse the attacking companies of acting at the behest of the U.S. Government. Employees of those companies residing in the complaining country may be arrested and held. Headlines are certain. In addition, foreign countries and companies will have a stronger legal basis for their complaints than just U.S. law. The U.S. has signed and ratified the [Council of Europe Convention on Cybercrime](http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

Impact: Lose enforcement of human rights and negative net benefits as the fabric of international law is undermined

Prof. David A. Koplow 2013 (law professor, Georgetown Univ.) Indisputable Violations: What Happens When the United States Unambiguously Breaches a Treaty? FLETCHER FORUM OF WORLD AFFAIRS, Winter 2013 <http://www.fletcherforum.org/wp-content/uploads/2013/02/Koplow_37-1.pdf>



5. Hype Will Backfire

Link: AFF hypes a “threat” with zero casualties. Public will suspect hype is a smokescreen for some other agenda

Robert M. Lee & Prof. Thomas Rid 2014. (Lee is an active-duty US Air Force Cyber Warfare Operations Officer who has led multiple cyberspace operations programmes in the Air Force and US Intelligence Community. Rid is a professor in the Department of War Studies at King's College London) Oct 2014 The RUSI JOURNAL Vol 159 Issue 5 “OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy” <http://www.tandfonline.com/doi/full/10.1080/03071847.2014.969932#tabModule>

Hype damages the public's trust and confidence in the Internet and, ultimately, in their own governments. Inter-state conflict makes the public uneasy. Tension between states has a real social and economic impact. It is easy to see Russian troops invading Crimea on television and it would also be possible to see Russian troops withdrawing from Crimea. This visually defined ‘beginning’ and ‘end’ to events lessens tension and public concern. However, there is no visible beginning or end to cyber-conflict. Instead, the public relies on what it hears from governments, journalists, academia and industry; and their message is loud and clear: the grid could be hacked at any time, the lights could go out, financial markets could collapse, bank accounts could be raided, competitiveness could be lost to China. Some of these scenarios are certainly possible; but this constant barrage is sowing fear, uncertainty and doubt – ‘FUD’, in the jargon. When the predicted calamity seemingly does not happen, doubters instead start to wonder if the FUD could perhaps be a smokescreen for something else.

Link: Excess hype will actually reverse public support for cyber security

Robert M. Lee & Prof. Thomas Rid 2014. (Lee is an active-duty US Air Force Cyber Warfare Operations Officer who has led multiple cyberspace operations programmes in the Air Force and US Intelligence Community. Rid is a professor in the Department of War Studies at King's College London) Oct 2014 The RUSI JOURNAL Vol 159 Issue 5 “OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy” <http://www.tandfonline.com/doi/full/10.1080/03071847.2014.969932#tabModule>

The US and UK governments and intelligence agencies actually have a convincing response: do not speculate, they say – your evidence is not good, pay attention to details and do not overstate the problem. However, the governments’ propensity to do the same thing themselves with regard to cyber-security – to speculate, generate hype and ignore the finer detail – has led rightfully frustrated citizens to lose trust in their elected officials. This careless attitude towards public support is now biting back.

Impact: Turn the harms. Cyber security efforts will crash

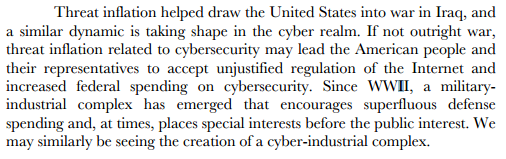
Robert M. Lee & Prof. Thomas Rid 2014. (Lee is an active-duty US Air Force Cyber Warfare Operations Officer who has led multiple cyberspace operations programmes in the Air Force and US Intelligence Community. Rid is a professor in the Department of War Studies at King's College London) Oct 2014 The RUSI JOURNAL Vol 159 Issue 5 “OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy” <http://www.tandfonline.com/doi/full/10.1080/03071847.2014.969932#tabModule>

Today the hype machine has full momentum; it practically controls the debate – and it is self-defeating. In a democracy, government, the press, academia and industry are supposed to keep each other in check, to balance each other. Political opposition, editorial fact-checking, scholarly peer review and business competition should calibrate output and lead to progress over time. Old-fashioned cyberneticists and control engineers call this *negative feedback*. It is what creates stable systems and balance, keeping machines humming steadily instead of pushing them into overdrive. Cyber-hype has created a culture without checks and balance – it is *positive feedback*, in engineering lingo, pushing systems to overheat or overpressure, and finally to crash.

6. Wasted money

Link: Inflating the cyber war threat leads to higher unnecessary federal spending

Jerry Brito & Tate Watkins 2011. (Brito - was a senior research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program. He also serves as an adjunct professor of law at George Mason University. Watkins - was a research associate for the Technology Policy Program and the State and Local Policy Project.) 26 Apr 2011 Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy <http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy-0>



Impact: Every increase in the deficit hurts the economy

Dr William Gale and Benjamin Harris 2011. (Gale - PhD in economics, Stanford Univ.; senior fellow at the Brookings Institution and co-director of the Urban-Brookings Tax Policy Center; former assistant professor in the Department of Economics at UCLA, and a senior economist for the Council of Economic Advisers under President George H.W. Bush; Harris - master’s degree in economics from Cornell University and a master’s degree in quantitative methods from Columbia University; senior research associate with the Economics Studies Program at the Brookings Institution) “A VAT for the United States: Part of the Solution” <http://www.taxanalysts.com/www/freefiles.nsf/Files/GALE-HARRIS-5.pdf/$file/GALE-HARRIS-5.pdf>

But even in the absence of a crisis, sustained deficits have deleterious effects, as they translate into lower national savings, higher interest rates, and increased indebtedness to foreign investors, all of which serve to reduce future national income. Gale and Orszag (2004a) estimate that a 1 percent of GDP increase in the deficit will raise interest rates by 25 to 35 basis points and reduce national saving by 0.5 to 0.8 percentage points of GDP. Engen and Hubbard (2004) obtain similar results regarding interest rates.

Works Cited: Hack Back (NEG)

1. Dr Jon R. Lindsay 2014. The Impact of China on Cybersecurity: Fiction and Friction <http://belfercenter.ksg.harvard.edu/files/IS3903_pp007-047.pdf>
2. Dr William Gale and Benjamin Harris 2011. “A VAT for the United States: Part of the Solution” <http://www.taxanalysts.com/www/freefiles.nsf/Files/GALE-HARRIS-5.pdf/$file/GALE-HARRIS-5.pdf>
3. Dr. Ted Galen Carpenter 2004. 10 Aug 2004, "China's Taiwan Policy and America's Difficult Choices" <http://www.cato.org/pub_display.php?pub_id=2778>
4. Emilio Iasiello 2015. “Ramping Down Chinese Commercial Cyber Espionage” FOREIGN POLICY JOURNAL 9 Dec 2015 <http://www.foreignpolicyjournal.com/2015/12/09/ramping-down-chinese-cyber-espionage/>
5. Greg Austin 2013. 26 Sept 2013 China’s Cyber Espionage Priorities <http://ewipolicy.tumblr.com/post/62325267109/chinas-cyber-espionage-priorities>
6. Jerry Brito & Tate Watkins 2011. 26 Apr 2011 Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy <http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy-0>
7. Jody Westby 2012. FORBES magazine 29 Nov 2012 “Caution: Active Response to Cyber Attacks Has High Risk” <http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/#335808882cd0>
8. Lance Deviney 2014. TOP CYBER: DEVELOPING THE TOP ONE PERCENT TO DEFEAT THE ADVANCED PERSISTENT THREAT 13 Feb 2014 <http://www.au.af.mil/au/awc/awcgate/awc/2014_deviney.pdf>
9. Lauren Weinstein 2013. 24 May 2013 “USA Intellectual Property Theft Commission Recommends Malware!” <http://lauren.vortex.com/archive/001034.html>
10. Loras R. Evans 2000. Intrusion Detection FAQ: What is a Honeypot? <https://www.sans.org/security-resources/idfaq/honeypot3.php>
11. Micah Zenko 2014. FOREIGN POLICY, “Exaggeration Nation” 21 Nov 2014 <http://foreignpolicy.com/2014/11/21/exaggeration-nation/?wp_login_redirect=0>
12. Michael Riley and Ben Elgin 2013. BLOOMBERG NEWS 2 May 2013 “China’s Cyberspies Outwit Model for Bond’s Q” <http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html>
13. Mike Masnick 2013. 28 MAY 2013 Fear Mongering Report Suggests 'IP Theft From China' One Of The Biggest Problems America Faces <https://www.techdirt.com/articles/20130526/22281723217/fear-mongering-report-suggests-ip-theft-china-one-biggest-problems-america-faces.shtml>
14. Prof. David A. Koplow 2013. Indisputable Violations: What Happens When the United States Unambiguously Breaches a Treaty? FLETCHER FORUM OF WORLD AFFAIRS, Winter 2013 <http://www.fletcherforum.org/wp-content/uploads/2013/02/Koplow_37-1.pdf>
15. Prof. Jack Goldsmith 2013. 10 Oct 2013 “We Need an Invasive NSA” THE NEW REPUBLIC <http://www.newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks>
16. Robert M. Lee & Prof. Thomas Rid 2014. Oct 2014 The RUSI JOURNAL Vol 159 Issue 5 “OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy” <http://www.tandfonline.com/doi/full/10.1080/03071847.2014.969932#tabModule>