Chinese Hackers? US Propagandists Should Look in the Mirror

Like millions of Americans, this past week I was sitting on my couch, drinking a cold beer, watching Game 1 of the World Series – professional baseball’s hallowed championship. Suddenly the satellite feed went out, the screen went dark. Naturally, as FOX Sports scrambled to get their live feed fixed, many of my fellow Americans took to twitter to speculate as to what had caused the outage. I was, sadly, unsurprised to see that the most common joke people were making was that China must have hacked the World Series.

On the one hand, it is understandable given the barrage of propaganda about Chinese hackers as a threat to corporate and national security; seemingly every week there is a new news item highlighting the great red cyber-menace. On the other hand, it is a perfect illustration of the hypocrisy and ignorant arrogance of Americans who, despite being citizens of unquestionably the most aggressive nation when it comes to both cyber espionage and surveillance, see fit to cast China as the real villain. It is a testament to the power of both propaganda and imperial triumphalism that a proposition so disconnected from reality, and bordering on Orwellian Doublethink, is not only accepted, but is ipso facto true.

But there is a deeper political and sociological phenomenon at play here, one that begs further exploration. How is it that despite all the revelations of Edward Snowden regarding US intelligence and military snooping capabilities across the globe, Americans still cannot accept the culpability of their own government and corporate interests – the two work hand in hand – in global cyber-espionage? Even if they explicitly or implicitly know about the NSA, CIA, DIA, and Pentagon programs (among many others), their instinctive reaction is to blame China. Why? The answer lies in the complexity and effectiveness of the anti-China propaganda.

In his landmark book Public Opinion, the renowned writer, commentator, and theoretician of propaganda, Walter Lipmann, defined the term “stereotype” in the modern psychological sense as a “distorted picture or image in a person’s mind, not based on personal experience, but derived culturally.” In other words, the stereotype is an image in our mind’s eye, one that is constructed by outside forces; it is information filtered through a particular societal or cultural framework that then creates a picture of how something is to be understood. Lipmann went further, noting that carefully constructed propaganda could be used to shape stereotypes, thereby allowing the powers that be the ability to construct and manipulate information and narratives.

And this is precisely the phenomenon at work here. By repeating it endlessly, the US political and corporate media establishment have successfully convinced Americans that China is the real threat when it comes to cyberspace, playing on the stereotype of Chinese people in general, and the People’s Republic of China specifically. But, I would argue something far different: rather than seeing China as a threat, perhaps Americans, and westerners generally, should shine a light on what their own countries are doing, thereby gaining a broader perspective on the issue. For China’s moves in this field pale in comparison to those of the US, and are clearly a response to them.

China and the US: Comparing the Rap Sheets

The corporate media is replete with stories of Chinese hacking of US institutions. From alleged Chinese hacking of the University of Virginia employees connected with US government programs directed at China, to the infamous breach of the federal government’s Office of Personnel Management which resulted in the theft of the personal
information of more than 20 million Americans, such stories help to construct an image of China as the world’s leading hacker-state. This week it is Chinese hackers targeting health care providers, last year it was stealing the secrets of Westinghouse and US Steel, and literally dozens of other such examples.

The purpose of this article is not to deny the veracity of these reports; I’m not a computer expert, nor do I have access to the information that an expert would need in making a determination. Instead, my purpose here is to show the grossly unbalanced, and utterly dishonest, way in which the issue is presented to Americans especially, and to probe why that might be. For any fair and balanced approach to the issue would present the simple fact that the US is the world leader in cyber-warfare, having actually conducted what are to date the only recorded live uses of cyberweapons.

Take for instance the joint US-Israel developed Stuxnet virus, a pair of highly complex and severely destructive, computer viruses launched at Iran’s nuclear facilities. According to a group of independent legal experts assembled at the request of NATO’s Cooperative Cyber Defense Center of Excellence, the Stuxnet cyberattack was “an act of force.” Their report noted that “Acts that kill or injure persons or destroy or damage objects are unambiguously uses of force [and likely violate international law].”

Indeed, the US and its Israeli partners launched the very first true cyberweapon. As cyber security expert Ralph Langer wrote in Foreign Policy in 2013:

> Stuxnet is not really one weapon, but two. The vast majority of the attention has been paid to Stuxnet’s smaller and simpler attack routine — the one that changes the speeds of the rotors in a centrifuge, which is used to enrich uranium. But the second and “forgotten” routine is about an order of magnitude more complex and stealthy. It qualifies as a nightmare for those who understand industrial control system security...The “original” payload...attempted to overpressurize Natanz’s centrifuges by sabotaging the system meant to keep the cascades of centrifuges safe.

Essentially, the US and Israel employed the world’s first cyberweapon without even fully knowing the potentially destructive consequences. As the virus migrated out of the Iranian nuclear facility at Natanz and onto the internet, innumerable variables could have come into play, with the potential for disastrous outcomes.

But of course Stuxnet was not alone. The US and Israel also deployed both the Gauss and Flame viruses, two more sophisticated cyberweapons designed to cause major damage to online infrastructure. The Gauss virus, discovered by Kaspersky labs, one of the world’s most highly respected cyber-security firms, was designed to steal sensitive data such as financial records. According to the US officials who spoke with the Washington Post, the Flame virus was a:

> massive piece of malware [which] secretly mapped and monitored Iran’s computer networks, sending back a steady stream of intelligence to prepare for a cyber[warfare campaign]... “This is about preparing the battlefield for another type of covert action... Cyber-collection against the Iranian program is way further down the road than this.” said one former high-ranking U.S. intelligence official, who added that Flame and Stuxnet were elements of a broader assault that continues today.

Clearly the US and Israel were not merely interested in surveillance and information-gathering, but actually having the ability to manipulate and destroy vital computer infrastructure in Iran. Any reasonable reading of international law should hold that such actions are, in fact, an act of war, though of course war with Iran has not come to pass. But just the very use of such sophisticated weapons, far more elaborate, technical, and dangerous than mere hacking by humans, should call into question the weepy-eyed condemnations of China for its alleged stealing of corporate and government information.

And then of course there is the seemingly endless supply of revelations from Edward Snowden regarding the US surveillance infrastructure, how all-encompassing it truly is, how it is used to manipulate political outcomes, how it is used as a weapon against foreign governments, and much more.

Just to name a few of the countless programs and initiatives of the NSA and the surveillance state designed to capture information for political purposes:

- **PRISM** – allows “The National Security Agency and the FBI [to tap] directly into the central servers of nine leading U.S. internet companies, extracting audio and video chats, photographs, emails, documents, and connection logs.”
- **BLARNEY** – “Gathers up metadata from choke points along the backbone of the internet as part of an ongoing
collection program the leverages IC (intelligence community) and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks.”

- **Boundless Informant** – “Details and even maps by country the voluminous amount of information it collects from computer and telephone networks.”
- **US & UK Target G20 Leaders** – “The documents suggest that the operation was sanctioned in principle at a senior level in the government.”
- **US Spied on EU Offices** – “America’s National Security Agency (NSA) not only conducted online surveillance of European citizens, but also appears to have specifically targeted buildings housing European Union institutions... in addition to installing bugs in the building in downtown Washington, DC, the European Union representation's computer network was also infiltrated.”

But of course, the US has also specifically, and successfully, trained its cyber-espionage and cyber-warfare sights on China itself. Thanks to Snowden, we now know that US intelligence repeatedly hacked into Beijing’s Tsinghua University, China’s top education and research institute. As revealed in the South China Morning Post:

> The information also showed that the attacks on Tsinghua University were intensive and concerted efforts. In one single day of January, at least 63 computers and servers in Tsinghua University have been hacked by the NSA...The university is home to one of the mainland’s six major backbone networks, the China Education and Research Network (CERNET) from where internet data from millions of Chinese citizens could be mined. The network was the country’s first internet backbone network and has evolved into the world’s largest national research hub.

But it wasn’t only Tsinghua University that was targeted. Snowden also revealed that Chinese University in Hong Kong was the victim of US hacking; the university is home to the Hong Kong Internet Exchange, the city’s central hub for all internet traffic. In addition, it came out that US intelligence has repeatedly hacked into Chinese mobile phone companies, spied on users, and stolen data, including text messages. These are, of course, only what we know about thus far from the Snowden revelations. The scope of US hacking operations against China is not known, but could be safely assumed to be far-reaching.

In fact, the depth of US hacking and other intelligence operations targeting China, including those taking place inside China itself, has been alluded to repeatedly. The New York Times noted in August 2015 that the Obama administration was cautious about any retaliation against China for the breach of the Office of Personnel Management because “Intelligence officials say that any legal case could result in exposing American intelligence operations inside China — including the placement of thousands of implants in Chinese computer networks to warn of impending attacks.”

It is clear that what we do know about US cyberwar programs and tactics is really only the tip of the iceberg. It is likely that Washington has myriad other China-specific hacking programs and initiatives, including the much discussed attempts to subvert the oft referenced “Great Firewall of China.” Put simply, the US is engaged in the most sophisticated forms of hacking and cyber-subversion, and much of it is directed at China (and Russia and Iran). This should now be beyond question.

Keep this information in mind the next time another story about Chinese hackers attacking US interests runs in the corporate media. While the hack may or may not be true, it is the context within which such actions take place that really needs to be understood.

There is a cyberwar going on, of this there can be no doubt. But who’s got the biggest guns? And who fired the first shot?

---

**Eric Draitser is an independent geopolitical analyst based in New York City, he is the founder of StopImperialism.org and OP-ed columnist for RT, exclusively for the online magazine “New Eastern Outlook”**.