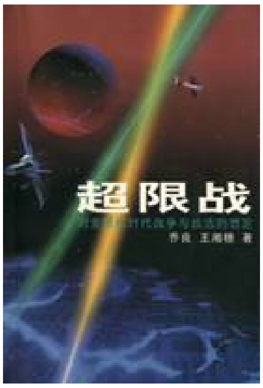
WHY SO SURPRISED? CIA, U.S. MILITARY KNEW CHINESE HACKERS EXPECTED SINCE 1999



Cover, Unrestricted Warfare via Wikimedia

The breathless reporting about the alleged Chinese hacking at The New York Times is truly annoying because of the shock it displays. The surprise any major government or private corporate entity shows at this point about any network-based security breach that appears to originate from China should be treated as propaganda, or a display of gross ignorance.

In 1999, the CIA's Foreign Broadcast Information Service published a white paper entitled Unrestricted Warfare, written by the PRC's Col. Qiao Liang and Col. Wang Xiansui. The publication outlined the methodologies a nation-state could deploy as part of an asymmetric war. Further, the same work outlined the U.S.'s weaknesses at that time were it to confront such asymmetric warfare. It did not focus any other nation-state, just the U.S.*

The colonels acknowledged that the U.S.–at the time of the paper–had considered using a range of tools in response to conflicts:

> “…There’s no getting around the opinions of the Americans when it comes to discussing what means and methods will be used to fight future wars. This is not simply because the U.S. is the latest lord of the mountain in the world. It is more because the opinions of the Americans on this question really are superior compared to the prevailing opinions among the military people of other nations. The Americans have summed up the four main forms that warfighting will take in the future as: 1) Information warfare; 2) Precision warfare [see Endnote 8]; 3) Joint operations [see Endnote 9]; and 4) Military operations other than war (MOOTW) [see Endnote 10]. This last sentence is a mouthful. From this sentence alone we can see the highly imaginative, and yet highly practical, approach of the Americans, and we can also gain a sound understanding of the warfare of the future as seen through the eyes of the Americans. Aside from joint operations, which evolved from traditional cooperative operations and coordinated operations, and even Air-Land operations, the other three of the four forms of warfighting can all be considered products of new military thinking. General Gordon R. Sullivan, the former Chief of Staff of the U.S. Army, maintained that information warfare will be the basic form of warfighting in future warfare. For this reason, he set up the best digitized force in the U.S. military, and in the world. Moreover, he proposed the concept of precision warfare, based on the perception that “there will be an overall swing towards information processing and stealthy long-range attacks as the main foundations of future warfare.” For the Americans, the

> advent of new, high-tech weaponry, such as precision-guided weapons, the Global Positioning System (GPS), C4I systems and stealth airplanes, will possibly allow soldiers to dispense with the nightmare of attrition warfare. …”

The rise of military tools like drones for precision-guided stealth attacks was predicted; quite honestly, the PRC’s current cyber warfare could be a pointed response to Gen. Sullivan’s statement about information warfare.

But in acknowledging the U.S.’s future use of MOOTW, the colonels also offered up the most likely approaches in an asymmetric assault or response: trade war, financial war, new terror war in contrast to traditional terror war, ecological war. Of these, they cited a specific example of new terror war entity and attacks:

> “…In contradistinction to masked killers that rely on the indiscriminate slaughter of innocent people to produce terror, the “Falange Armed Forces”[…] group in Italy is a completely different class of high-tech terrorist organization. Its goals are explicit and the means that it employs are extraordinary. It specializes in breaking into the computer networks of banks and news organizations, stealing stored data, deleting programs, and disseminating disinformation. These are classic terrorist operations directed against networks and the media. This type of terrorist operation uses the latest technology in the most current fields of study, and sets itself against humanity as a whole. We might well call this type of operation “new terror war.”…

Note in particular that these Chinese military experts refer to attacks not on military targets, but on banks *and the media*.

Furthermore, the U.S. military could have predicted the Chinese investment in information warfare, as a paper Operation Allied Force: The View from Beijing, by Dr. James D. Perry (2000) noted. Perry had already absorbed the paper, Unrestricted Warfare:

> "…Two senior PLA officers observed that NATO's "asymmetrical" strikes employed "a number of new combat modes." Allied Force consisted of "a series of informationalized, digitized, and networked combat operations that surpassed those in the Gulf War." In their view, networked fighting centers will replace individual fighting platforms in future warfare, and networked military organizations will replace "tree-shaped" military organizations. The United States uses air raids, EW, and information-control operations to maximize the asymmetric advantages of its high technology. Therefore, the PLA should "learn and master" anti-air-raid, anti-electronic-warfare, and anti-information-control operations. …"

Perry also noted contributor Ye Lu of the state-owned Keji Ribao science and technology publication reported:

> "…the US goal is to gain mastery of battlefield information and that the information enhancement of US weapons systems is already "an order of magnitude" greater than in the Gulf War. Before initiating combat,
>
> *'reconnaissance satellites, relay satellites, high-altitude reconnaissance aircraft, and low- and medium-altitude pilotless aircraft of all kinds are to be deployed in continuous, uninterrupted, all around, dynamic intelligence reconnaissance against military and civilian targets in*

> *Yugoslavian territory . . . while at the same time numerous intelligence organizations and every means of intelligence collection are to be marshaled to conduct repeated position fixing and simulated attack exercises against all military and non-military targets that might be encountered in the battlefield to come.’20*
>
> Ye considered that despite all its advantages, the United States did not gain “information supremacy” in Yugoslavia. This he attributed to the expansion of the information domain through radio and computer networks that enable “both aggressors and defenders to attack and counterattack to the best of their abilities.” Ye drew the following conclusions from Allied Force:
>
> - *China should research and develop high-tech precision weapons and should upgrade the information systems associated with existing weapons.*
> - *China should develop IW equipment and techniques, especially those that can “reliably put constraints on the power of hostile forces.”*
> - *China needs a “corps of knowledgeable and experienced military information security personnel.”*

> - *China should create her own software for national defense and should find military applications for civilian high technologies.21 …”*

Again, the Chinese not only predicted the emergence of drone usage by the U.S., but spelled out a countervailing response including development of information technology for its national security.

The same report by Ye Lu, cited by Dr. Perry and published in a U.S. Air Force-Air University journal, was itself published by the CIA’s FBIS. Clearly both our military and our intelligence agency have been on notice for over a decade about China’s intentions with regard to cyber warfare.

We were warned; it could not be spelled out any more clearly. Not to mention other sources of intelligence, our government was handed a manual that not only laid out the likely routes of attack, including network-based assaults, but generously a description of the opportunities for improvement the U.S. should address to protect itself against non-traditional attacks, let alone improve the prospects to conduct assaults of their own in a similar fashion.

Granted, the document also suggests a unified structure for the U.S. or other nation-state to respond to all asymmetric attacks. This offering should be avoided for this reason—the unexpected is the element that offers the best chance to defend against non-traditional warfare.

But to have no organized response at all is absurd. In its absence we’re left with a choice of which mask we should adopt in reaction to attacks: the “We’ve got this” fakery, or an open admission of ignorance and failure—or perhaps both.

One more point we should note is the Chinese response by foreign minister’s office spokesman Hong Lei in state-owned Xinhua News to the NYT’s report:

> “Groundless criticism is irresponsible and unprofessional, and it will not help to solve the problem,” he said.

The infosecurity company Mandiant employed by NYT and the U.S., which had traced the source of the alleged hacking to a People’s Liberation Army site, took this as an insult to their conduct and went public with their findings.

But was the response really aimed at Mandiant? Or was it aimed at other government and private corporate targets warned clearly more than a decade ago?

* *Word analysis of the document published at Cryptome:*
“U.S.” appears 220 times; “Europe” appears 22 times; “Russia” appears 31 times, “China” appears 34 times. Occurrences counted in both text’s body and in footnotes.