US indictments offer window into Chinese intelligence operations

[Content preview – Subscribe to **Jane's Intelligence Review** for full article]

US criminal indictments are a valuable source on the activities of adversary intelligence agencies. *Neil Ashdown* examines how these indictments can support open-source analysis of Chinese intelligence operations

Key Points

- US government indictments of Chinese nationals accused of espionage provide a valuable source of information on Chinese intelligence operations.
- There are limits to the information likely to be presented in indictments, with a high likelihood of omissions and obfuscation related to US intelligence capabilities.
- Analysis of three cases of alleged Chinese espionage has led *Jane's* to assess with a high degree of confidence that at least two of the cases are connected.

On 20 December 2018, the UK and US governments accused two Chinese nationals associated with the Ministry of State Security (MSS) of conducting a wide-ranging hacking campaign aimed at stealing intellectual property, confidential business information, and technological information. The US Department of Justice (DoJ) issued indictments against Zhu Hua and Zhang Shilong, described as members of the hacking group termed APT10 by security researchers.

The DoJ statement claimed that the two had "acted in association with" the Tianjin State Security Bureau of the MSS. The UK Foreign and Commonwealth Office issued a statement saying that "the UK government has made the judgement that the Chinese Ministry of State Security was responsible", and noting that "[t]his is the first time that the UK government has publicly named elements of the Chinese government as being responsible for a cyber campaign".

In Senate testimony on 12 December 2018, US Assistant Attorney General John C Demers noted that between 2011 and 2018 "more than 90 percent of the Department [of Justice]'s cases alleging economic espionage by or to benefit a state involve[d] China". Demers is the leader of the US government's China Initiative, announced by then US attorney general Jeff Sessions on 1 November 2018. Sessions said, "Chinese economic espionage against the United States has been increasing – and it has been increasingly rapidly … We're not going to take it anymore."

Assessments of China's intelligence operations are a requirement for analysts, including those working in open sources. Criminal indictments (and similar documents such as criminal complaints) are a valuable unclassified source; they are generally more detailed than anything that appears outside declassified archival documents and are far more current.

US Deputy Attorney General Rod Rosenstein speaks at a news conference to announce the indictments against two Chinese hackers at the DoJ in Washington. The DoJ is at the centre of the US government's efforts to tackle Chinese espionage. (Alex Wong/Getty Images)

1728387

Similarly, on 13 July 2018, the investigation led by Special Counsel Robert Mueller indicted 12 Russian operatives of the military Main Intelligence Directorate (Glavnoye razvedyvatelnoye upravleniye: GRU) for conducting "large-scale cyber operations to interfere with the 2016 U.S. presidential election". Then, on 4 October, the DoJ announced charges against a further seven Russian military intelligence officers "for computer hacking, wire fraud, aggravated identity theft, and money laundering".

Such documents provide useful information about Chinese and Russian intelligence operations and – by extension – about US intelligence and counterintelligence capabilities. In a post on 13 July, the Lawfare blog noted that Mueller's indictment of the Russian intelligence officers "provides a great deal of information about the extent and internal

structure of the Russian government side of the 2016 hacking operation" and also that it "shows a massive, and successful, counterintelligence operation by the US government".

Source evaluation

China scholar and former intelligence officer Peter Mattis detailed the benefits of using criminal cases to understand intelligence operations in his 2011 thesis 'Chinese Intelligence Operations Reconsidered: Toward a New Baseline'. Mattis stated, "Without access to internal documents and former PRC [People's Republic of China] intelligence officers, espionage cases are the only way to get a sense of how the PRC intelligence services operate in practice."

Moreover, indictments are reliable sources. As Mattis noted, "especially in countries under the rule of law, [espionage cases] hold the most concrete information available, because court documents undergo an additional layer of scrutiny relating to the integrity of the data itself". Speaking to *Jane's* in December 2018, Mattis said, "These simply are the most reliable sources." He added that indictments provided "often definitive starting points for further research. For open-source research to succeed, it needs firm pegs from which to start pulling threads."

Nicholas Eftimiades, lecturer in the Homeland Security Program at Penn State University and the author of *Chinese Intelligence Operations* (1994), told *Jane's* in December 2018 that the indictments showed "element[s] of China's intelligence tradecraft". For further research, Eftimiades said that access to court papers available through the US government's Public Access to Court Electronic Records (PACER) programme was necessary, but that this was "expensive to use, and most definitely not user-friendly".

Criminal indictments will often include accounts of the operational techniques used by foreign intelligence officers, as establishing that the defendants were practising intelligence tradecraft will generally be a key goal of the prosecution. In the case of human intelligence (HUMINT), indictments often provide details about cultivation techniques and covert communications channels, as part of the prosecution's attempt to establish motive and criminal intent on the part of the defendant. Eftimiades noted that "deception, or intent to hide a criminal act, is often an integral element of the indictment".

In the case of cyber espionage, indictments can provide details such as the pseudonyms of network operators, specific types of malware used, and descriptions of tactics, techniques, and procedures. The Lawfare blog described the Mueller indictment as "identifying the specific officers with hands on keyboards".

Obfuscation and omission

Although the purpose of criminal indictments makes them a valuable source, it also brings challenges for an analyst. Material made available in indictments is primarily intended to establish probable cause that a crime has been committed. Because this is a lower bar than establishing guilt beyond reasonable doubt, the indictment may not include all the information available to the investigating officers. Eftimiades told *Jane's* that indictments

"often lack conspirators, specific locations, and nuances such as the involvement of larger corporate or government entities".

In cases involving intelligence and counterintelligence, obfuscation over US intelligence capabilities is highly likely. In his 2012 book *Deception: Spies, Lies and How Russia Dupes the West* , journalist Edward Lucas analysed indictments released relating to the group of Russian illegals detained in the US in June 2010. Lucas noted that the indictments would have been intended to "crack the defence of those arrested … [but also] to cause maximum annoyance and confusion to the Russian side". Lucas assessed that this would involve "overstating what the American side didn't know, and understating what it did."

[Continued in full version…]

(953 of 2899 words)