CIVIC IDEA

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

CAPS unlock CENTRAL ASIAN POLICY STUDIES

PRC'S SECRET CYBERATTACKS

TBILISI
2024

In March 2024, the world's media outlets were inundated with reports of malicious cyber-attacks perpetrated by PRC-affiliated organizations/individuals targeting the democratic institutions and parliamentarians of the United Kingdom. The news of the cyber-attacks prompted coverage from various reputable sources, including CNN, BBC, the New York Times, the Guardian and etc.

"China hits back at US, UK for sanctions on espionage hacks as coordinated pressure on Beijing grows"

Source: https://edition.cnn.com/2024/03/26/china/china-cyber-hacking-accusations-intl-hnk/index.html

"UK imposes sanctions after Chinese-backed cyber-attacks"

Source: https://www.bbc.com/news/uk-politics-68654533

The New York Times

U.K. Accuses China of Cyberattacks Targeting Voter Data and Lawmakers

The British government believes China has overseen two separate hacking campaigns, including one that yielded information from 40 million voters.

"U.K. Accuses China of Cyberattacks Targeting Voter Data and Lawmakers"

Source: https://www.nytimes.com/2024/03/25/world/europe/uk-china-cyberattack-hacking.html

News | Opinion | Sport | Culture | Lifestyle — The Guardian

World UK Climate crisis Ukraine Environment Science Global development Football **Tech**

Hacking

Explainer

China cyber-attacks explained: who is behind the hacking operation against the US and UK?

Chinese hacking group APT 31 has been accused by UK and US officials of targeting critics of Beijing, while New Zealand's systems have also been attacked

China has been accused by the US, UK and New Zealand of targeting sensitive information with cyber

"China cyber-attacks explained: who is behind the hacking operation against the US and UK?"

Source: https://www.theguardian.com/technology/2024/mar/26/china-cyber-attack-uk-us-explained-hack-apt-31

According to the National Cyber Security Centre, in 2021-2022 UK institutions and parliamentarians were targets of various cyber-attacks. In August 2021 hostile cyber activities were detected in the electoral systems of the country. At the same time, the attacks were carried out against the UK Electoral Commission. However, the identities of the suspected individuals remained undisclosed. It is notable that the cyber-attackers had access to the personal data (the names and addresses) of nearly 40 million citizens of the UK who were registered to vote in Northern Ireland, Great Britain, and overseas. As stated by the Electoral Commission, these cyber-activities did not influence the UK elections' results.

Alongside the attack on the Electoral Commission, separate reconnaissance activities were conducted against the parliamentary accounts, according to the statement made by the UK's House of Commons on 25 March 2024. The attacks on parliamentarians' emails proved unsuccessful. Nevertheless, it is remarkable that the targets of the cyber campaigns were the individuals who openly criticized the PRC for its malicious political activities.

In response to the aforementioned cyber-attacks, the UK imposed sanctions on two Chinese nationals (Zhao Guangzong and Ni Gaobin) and a Chinese company („Wuhan Xiaoruizhi Science and Technology Company Ltd"). Also, the Chinese ambassador to the UK was summoned to account for the incidents.

After the cyber-attacks against the UK, the European Union issued a statement and called on China to fulfill its obligations within the UN framework of responsible state behavior in cyberspace. Precisely, the EU stated that the Chinese government should take action against the cyber-attacks undertaken from its territory.

Amid the growing cyber-threats of Chinese state-affiliated actors, 7 Chinese nationals were charged in the U.S. According to the indictment document, defendants (Ni Gaobin, Weng Ming, Cheng Feng, Peng Yaowen, Sun Xiaohui, Xiong Wang, Zhao Guangzong) were members of the cyberespionage program functioning within the Hubei State Security Department. The group is known as "Advanced Persistent Threat 31" ("APT31") by cybersecurity researchers. Remarkably, the individuals accused of the electronic intrusions against the UK parliamentarians and institutions are connected to the mentioned group.

The investigation uncovered a pattern of cyberattacks dating back to 2010, perpetrated by members of APT31 targeting U.S. officials, activists, academics, members of Congress, as well as various economic and defense industries. In response, the U.S. Department of the Treasury imposed sanctions on two defendants. Additionally, the U.S. Department of State announced a $10 million reward for information on the accused individuals, their affiliated organizations, or associated entities.

The members of the APT31 group used messages with secret tracking links to attack their targets. These electronic messages were purported to be from leading media outlets (such as, CNN, and Vox) or famous journalists. In the case of opening the electronic message, information about the recipient (the location, IP addresses, specific devices with access to the email accounts, etc.) was transmitted to a server controlled by the cyber-attackers. Followingly, the members of APT31 used this information to undertake more intricate and targeted cyber assaults. Between June and September 2018, over 10,000 malicious tracking emails were dispatched to senior U.S. officials and their advisors.

The cyber-attacks targeted members of the Senate, representatives from both the Republican and Democratic Parties, and those U.S. officials, who were employed at the White House, the Departments of Justice, Commerce, Treasury, and State. There were cases of malicious cyber-activities against the spouses of high-ranking U.S. officials as well. It is noteworthy that the election campaign staff of the U.S. political parties were also among the victims. Namely, in 2021, the Inter-Parliamentary Alliance on China ("IPAC"), dedicated to addressing anti-democratic actions and threats from the Chinese Communist Party, found itself targeted by cyber-attacks.

Additionally, among the targeted audience of the computer network intrusion activities, were the companies/individuals, who operate in strategically significant fields, including defense, information technology, telecommunications, etc. The defendants also faced charges for cyber-attacks against entities openly opposing the anti-democratic policies of the PRC, such as Hong Kong democracy activists and their partners.

Consequently, the U.S. Intelligence Community stated in its annual threat assessment document that "the PRC may attempt to influence the U.S. elections in 2024 at some level" to foster U.S. societal divisions.

According to the indictment document of the U.S. court (of the eastern district of New York), the PRC conducted its intelligence activities through various institutions, including the Ministry of State Security („MSS"). The departments of the ministry seek to gather information about other countries' political, economic, and security policies and influence their foreign policy. For this reason, the ministry was engaged in espionage activities against many countries, including the U.S.

In 2010, the Hubei State Security Department (HSSD) established a front company named "Wuhan Xiaoruizhi Science & Technology Co., Ltd," formally, engaged in research and technology development. However, in reality, this company served as a vehicle for cyber-attacks orchestrated by the HSSD. Consequently, both the U.S. and the UK imposed sanctions on this entity.

It is worthy of attention that the individuals charged with cyber-attacks against the U.S. and the UK operated within the HSSD. This department was a provincial branch of the PRC Security Department.