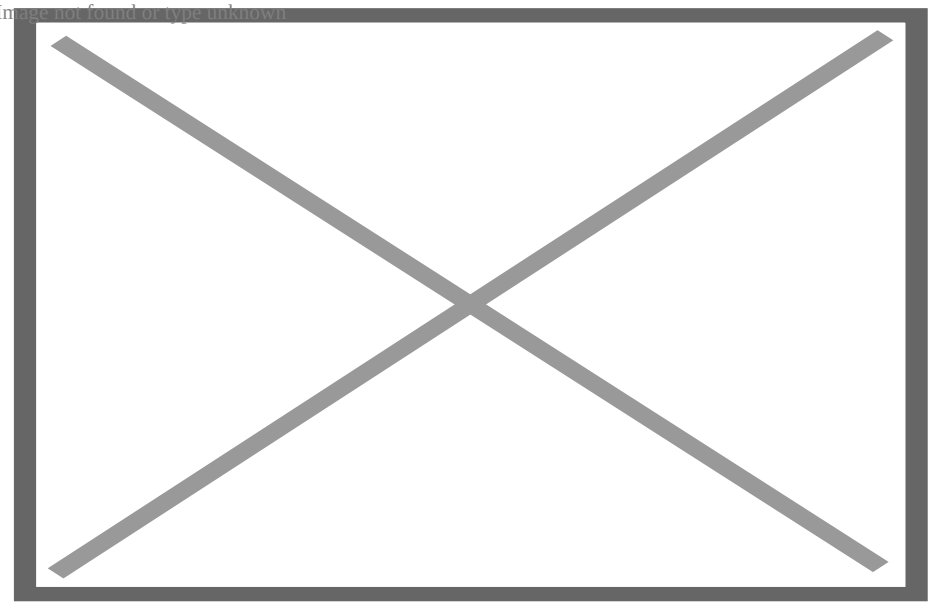
How CIA Schemes Color Revolutions Around the World

Description

by Yuan Hong via Global Times

Image not found or type unknown



cyber attack Photo:VCG

For a long time, the US Central Intelligence Agency (CIA) has plotted “peaceful evolution” and “color revolutions” as well as spying activities around the world. Although details about these operations have always been murky, a new report released by China’s National Computer Virus Emergency Response Center and Chinese cybersecurity company 360 on Thursday unveiled the main technical means the CIA has used to scheme and promote unrest around the world.

According to the report, since the beginning of the 21st century, the rapid development of the internet offered “new opportunity” for CIA’s infiltration activities in other countries and regions. Any institutions or individuals from anywhere in the world that use US digital equipment or software could be turned into the CIA’s “puppet agent.”

For decades, the CIA has overthrown or attempted to overthrow at least 50 legitimate governments abroad (the CIA has only recognized seven of these instances), causing turmoil in related countries. Whether it is the “color revolution” in Ukraine in 2014, the “sunflower revolution” in Taiwan island, China, or the “saffron revolution” in Myanmar in 2007, the “green revolution” in Iran in 2009, and other attempted “color revolutions” — the US intelligence agencies are behind them all, according to the report.

The US’ leading position in technologies of telecommunication and on-site command has provided unprecedented possibilities for the US intelligence community to launch “color revolutions” abroad. The

report released by the National Computer Virus Emergency Response Center and 360 disclosed five methods commonly used by the CIA.

The first is to provide encrypted network communication services. In order to help protesters in some countries in the Middle East keep in touch and avoid being tracked and arrested, an American company, which, reportedly, has a US military background, developed TOR technology that can stealthily access the internet — the Onion Router technology.

The servers encrypt all information that flows through them to help certain users to surf the web anonymously. After the project was launched by American companies, it was immediately provided free of charge to anti-government elements in Iran, Tunisia, Egypt and other countries and regions to ensure that those “young dissidents who want to shake their own government’s rule” can avoid the scrutiny of the government, according to the report.

The second method is to provide offline communication services. For example, in order to ensure that anti-government personnel in Tunisia, Egypt and other countries can still keep in touch with the outside world when the internet is disconnected, Google and Twitter quickly launched a special service called “Speak2Tweet,” which allows users to dial and upload voice notes for free.

These messages are automatically converted into tweets and then uploaded to the internet, and publicly released through Twitter and other platforms to complete the “real-time reporting” of the event on site, said the report.

The third method is to provide on-site command tools for rallies and parades based on the internet and wireless communications. The report noted that the US RAND Corporation has spent several years developing a non-traditional regime change technology called “swarming.” The tool is used to help a large number of young people connected through the internet join the “one shot for another place” mobile protest movement, greatly improving the efficiency of on-site command of the event.

The fourth is American developed software called “Riot.” The software supports 100 percent independent broadband network, provides variable WiFi network, does not rely on any traditional physical access method, does not need telephone, cable or satellite connection, and can easily escape any form of government monitoring.

The last one is the “anti-censorship” information system. The US State Department regards the research and development of the system as an important task and has injected more than $30 million into the project.

High vigilance needed

Moreover, the National Computer Virus Emergency Response Center and 360 company have spotted Trojan horse programs or plug-ins related to the CIA in recent cyberattacks targeting China. The public security authorities have investigated these cases, the Global Times has learned.

Aside from the five methods the CIA has used to incite unrest globally, through further technical analysis, the National Computer Virus Emergency Response Center and 360 company also identified another nine methods used by the CIA as “weapons” for cyberattacks, including attack moduledelivery, remote control, information collection and stealing, and third-party open-source tools.

The response center and 360 company also spotted an information-stealing tool used by the CIA, which is also one of the 48 advanced cyber weapons exposed in the confidential document of the US National Security Agency.

The discovery of these information-stealing tools shows that the CIA and the US National Security Agency will jointly attack the same victim, or share cyberattack weapons with each other, or provide relevant technical or human support, according to the report.

These new findings also offer important new evidence in tracing the identity of the APT-C-39 attackers. In 2020, 360 company independently discovered an APT organization that had never been exposed to the outside world, and named it APT-C-39. The organization specifically targets China and its friendly countries to carry out cyberattack and stealing activities, and its victims are spread all over the world.

The report also noted that the danger of CIA attack weapons can be glimpsed from third-party open-source tools as it often uses these tools to carry out cyberattacks.

The initial attack of the CIA cyberattack operation will generally be carried out against the victim’s network equipment or server. After obtaining the target purview, it will further explore the network topology of the target organization and move to other networked devices in the internal network to steal more sensitive information and data.

The controlled target computer is monitored in real time for 24 hours, and all information will be recorded. Once a USB device is connected, the private files in the victim’s USB device will be monitored and automatically stolen. When conditions permit, the camera, microphone and GPS positioning device on the user terminal will be remotely controlled and accessed, according to the report.

These CIA cyber weapons use standardized espionage technical specifications, and various attack methods echo and interlock and have now covered almost all internet and IoT assets worldwide, and can control other countries’ networks anytime, anywhere to steal important and sensitive data from other countries.

The American-style cyber hegemony is evident, the report notes.

Chinese Foreign Ministry spokesperson Mao Ning said on Thursday that US intelligence and espionage activities and cyberattacks on other countries deserve high vigilance from the international community.

The US must take seriously and respond to the concerns from the international community, and stop using cyber weapons to carry out espionage and cyberattacks around the world, Mao said.

In response to the highly systematic, intelligent, and concealed cyberattacks launched by the CIA against China, it is important for domestic government agencies, scientific research institutions,

industrial enterprises, and commercial organizations to quickly find out and deal with them immediately upon discovery, the report says.

The report suggests that in order to effectively deal with imminent network and real-world threats, while adopting self-controllable localized equipment, China should organize self-inspection against APT attacks as soon as possible, and gradually establish a long-term defense system to achieve comprehensive systematic prevention and control against advanced attacks.