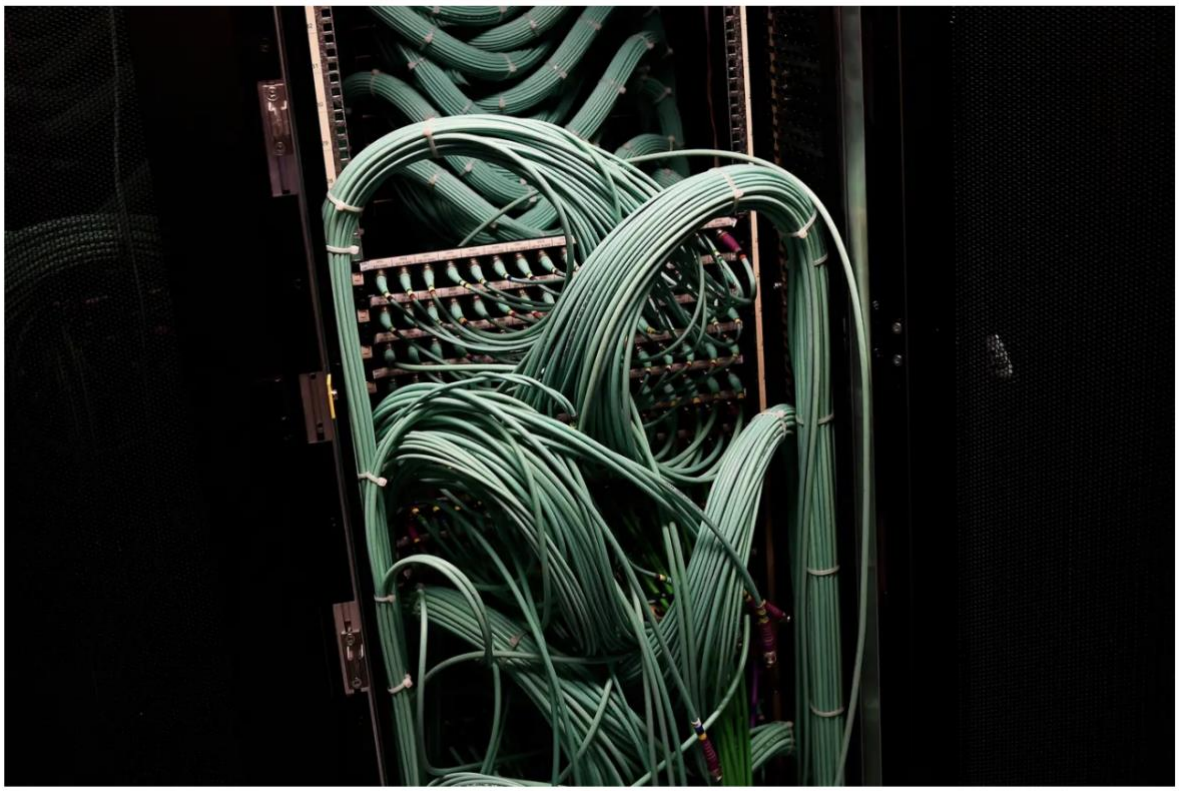
NZZ Artikel vom 11.2.2021

Den Cyberkrieg nicht eskalieren lassen



Dylan Martinez / Reuters

Den Kabelsalat zu ordnen, ist hilfreich, doch nicht die Lösung: Wie lassen sich aggressive Akteure im Cyberspace bändigen?

Der grossangelegte Cyberangriff auf die USA kommt einem Weckruf gleich. Wie man solch aggressive Akte verhindern kann und wie man ihnen begegnen soll, bleibt unklar. Gastkommentar von Paul Meyer und Daniel Stauffacher

Die USA sind jüngst Opfer eines Cyberangriffs erschütternden Ausmasses geworden: Mittels eines kompromittierten Software-Upgrades hatte sich ein ausländischer Akteur Zugang zu einer Vielzahl sensibler Daten verschafft. Über 18 000 Organisationen innerhalb und ausserhalb der Regierung hatten die Software installiert, und es dauerte sechs Monate, bis die Sicherheitslücke erkannt wurde.

Wie viele Daten entwendet wurden, wird sich nie exakt eruieren lassen. Die amerikanischen Verantwortlichen für Cybersicherheit stehen vor der gewaltigen Aufgabe, die unerwünschten Eindringlinge aus den Computersystemen zu entfernen und zu verhindern, dass die Angriffe im Verborgenen weitergehen. Die Attacke wurde extrem raffiniert durchgeführt, wie in einem Spionage-Thriller. Und genau das war es auch – ein Spionage-Akt, der aller Wahrscheinlichkeit nach vom russischen Auslandsgeheimdienst durchgeführt wurde.

Ex-Präsident Trump spielte die Bedeutung des Cyberangriffs jedoch herunter und unterstellt, dass nicht Russland, sondern China dafür verantwortlich sei. Die Haltung von Jon Biden ist kämpferischer. Er hat versprochen, dass die Verantwortlichen für ihre Taten bezahlen werden, und erklärt, dass eine gute Verteidigung nicht ausreiche: Die USA müssten ihre Gegner davon abhalten, solche Cyberangriffe überhaupt durchführen zu können. Der Aktivismus solcher Ansagen mag beruhigend wirken, birgt aber auch das Risiko einer weiteren Eskalation. Es bleibt unklar, was ein «signifikanter Cyberangriff» ist und wie eine verhältnismässige Reaktion genau aussehen müsste.

Bidens Aussage macht auch deutlich, dass der Begriff «Cyberangriff» oft pauschal eingesetzt wird. Es sollte künftig besser zwischen den Aktivitäten unterschieden werden; korrekter wäre, sie insgesamt als «offensive Cyberoperationen» zu bezeichnen.

Dabei sind drei Haupttypen zu identifizieren: Eine Computer Network Exploitation (CNE) ist eine Aktion, die

darauf abzielt, in ein fremdes Computersystem einzudringen und diesem Daten zu entnehmen, ohne dass die Betreiber des Systems dies merken. Eine Computer Network Attack (CNA) hat das Ziel, Daten im System zu stören, zu beschädigen oder sogar zu löschen. Informationsoperationen (IO) wiederum sind Cyberaktivitäten, die darauf abzielen, die Meinung der Bürger in einem Staat im Interesse eines angreifenden (staatlichen) Akteurs zu manipulieren.

Auch die Zivilgesellschaft und der private Sektor äussern zunehmend Besorgnis über unverantwortliche Handlungen staatlicher Akteure im Cyberspace. Dies unterstreicht die Notwendigkeit internationaler Zusammenarbeit. Um Cyberbedrohungen entgegenzutreten, muss für jeden der drei erwähnten offensiven Cyberangriffe eine geeignete Strategie formuliert werden. Die grösste Bedrohung für den zivilen Bereich stellen die CNA dar. Sie können wichtige öffentliche und zivile Dienste und Infrastrukturen beschädigen. Solche Attacken sind im Übrigen auch für die Angreifer schwer zu kontrollieren. Man denke an die Cyberoperationen «Not Petya» und «Wanna Cry» der letzten Jahre.

Der normative Rahmen, der die internationalen Cyberaktivitäten regeln soll, ist erst in Entwicklung. Seit 2015 hat man sich bei der Uno auf elf freiwillige Verhaltensnormen geeinigt. Erwähnenswert ist die Norm, die kritische öffentliche Infrastrukturen davor schützt, Ziel von Angriffen zu werden. Die Biden-Administration sollte sich für ein bilaterales amerikanisch-russisches (oder mit China sogar ein trilaterales) «Waffenstillstands»-Abkommen einsetzen, das für CNA-Operationen gelten würde.

Eine wachsende Bedrohung stellen auch Informationsoperationen dar, insbesondere weil sie eine massive Verbreitung von «Fake-News» ermöglichen. Internationale Übereinkünfte in diesem Bereich haben es schwer, denn die Propaganda des einen ist die Meinungsfreiheit des anderen. Nationale Regulierungen oder Kontrollmechanismen durch die Eigentümer von Social-Media-Plattformen stellen zumindest kurzfristig die praktikabelste Lösung dar. Langfristig wäre ein Verbot von Cyberoperationen anzustreben, die sich gegen Wahlinfrastruktur oder Wahlprozesse richten.

Bezüglich CNE ist wenig zu erwarten. Spionage ist ein bewährtes staatliches Mittel und hat sich bisher der Kontrolle der internationalen Gemeinschaft entzogen. 2015 hatten sich die USA und China auf eine Einschränkung des Cyberdiebstahls von geistigem Eigentum und Firmendaten geeinigt. Es wurde jedoch nach der Erhöhung der Spannungen nicht weitergeführt. Es ist anzunehmen, dass die US-Regierung keine Massnahmen unterstützen wird, die auch ihre eigenen ausländischen Cyberaktivitäten einschränken könnten.

Der Cyberspace ist unerlässlich für das Wohlergehen moderner Gesellschaften. Er ist jedoch anfällig für Missbrauch durch böswillige private Akteure sowie durch sich aggressiv gebärdende Staaten. Auf einen wirksamen Schutz vor Hacking kann nicht verzichtet werden.

Paul Meyer ist ehemaliger Botschafter von Kanada und ausserordentlicher Professor an der Simon-Fraser-Universität.

Daniel Stauffacher ist ehemaliger Delegierter des Bundesrats, Botschafter der Schweiz und Gründer des Think-Tanks ICT4Peace.

Aus dem NZZ-E-Paper vom 11.02.2021

Don't let the cyber war escalate

The large-scale cyberattack on the United States amounts to a wake-up call. How to prevent such aggressive acts and how to counter them remains unclear. Guest commentary by Paul Meyer and Daniel Stauffacher

The U.S. recently fell victim to a cyberattack of staggering proportions: Using a compromised software upgrade, a foreign actor had gained access to a large amount of sensitive data. More than 18,000 organizations inside and outside the government had installed the software, and it took six months for the vulnerability to be detected.

Exactly how much data was stolen will never be known. U.S. cybersecurity officials face the daunting task of removing the unwanted intruders from computer systems and preventing the attacks from continuing in secret. The attack was extremely sophisticated, like something out

of a spy thriller. And that's exactly what it was - an act of espionage, carried out in all likelihood by Russian foreign intelligence.

Ex-President Trump, however, downplayed the significance of the cyberattack, insinuating that China, not Russia, was responsible. Joe Biden's stance is more hawkish. He has promised that those responsible will pay for their actions, stating that a good defense is not enough: The U.S. must prevent its adversaries from being able to carry out such cyberattacks in the first place. The activism of such announcements may be reassuring, but it also risks further escalation. It remains unclear what constitutes a "significant cyberattack" and exactly what a proportionate response would need to look like.

Biden's statement also makes clear that the term "cyberattack" is often used sweepingly. In the future, there should be a better distinction between activities; it would be more correct to refer to them collectively as "offensive cyber operations."

Three main types should be identified: A Computer Network Exploitation (CNE) is an action that aims to penetrate and extract data from a foreign computer system without the operators of the system being aware of it. A Computer Network Attack (CNA) aims to disrupt, damage or even delete data in the system. Information Operations (IO), on the other hand, are cyber activities that aim to manipulate the opinion of citizens in a state in the interest of an attacking (state) actor.

Civil society and the private sector are also increasingly expressing concern about irresponsible actions by state actors in cyberspace. This underscores the need for international cooperation. To counter cyberthreats, an appropriate strategy must be formulated for each of the three offensive cyberattacks mentioned above. CNAs pose the greatest threat to the civilian sector. They can damage critical public and civilian services and infrastructure. Such attacks, moreover, are also difficult for the attackers to control. Consider the "Not Petya" and "Wanna Cry" cyber operations of recent years.

The normative framework to regulate international cyber activities is only in development. Since 2015, eleven voluntary norms of conduct have been agreed upon at the UN. Of note is the norm that protects critical public infrastructure from becoming a target of attack. The Biden Administration should advocate for a bilateral U.S.-Russian (or with China, even a trilateral) "ceasefire" agreement that would apply to CNA operations.

Information operations also pose a growing threat, particularly because they enable massive dissemination of "fake news." International agreements in this area are struggling because one person's propaganda is another's freedom of expression. National regulations or control mechanisms by the owners of social media platforms are the most viable solution, at least in the short term. In the long term, the goal would be to ban cyber operations that target election infrastructure or processes.

With respect to CNE, little can be expected. Espionage is a proven state tool and has so far escaped the scrutiny of the international community. In 2015, the U.S. and China had agreed to curb cyber theft of intellectual property and corporate data. However, it was not pursued after tensions rose. It is likely that the U.S. government will not support measures that could also restrict its own foreign cyber activities.

Cyberspace is essential to the well-being of modern societies. However, it is vulnerable to abuse by malicious private actors as well as by aggressively behaving states. Effective protection against hacking cannot be dispensed with.

Paul Meyer is former ambassador of Canada and associate professor at Simon Fraser University.

Daniel Stauffacher is a former Delegate of the Swiss Federal Council, Ambassador of Switzerland and founder of the think tank ICT4Peace.

From the NZZ e-paper of 11.02.2021

Translated with www.DeepL.com/Translator (free version)

Translated with www.DeepL.com/Translator (free version)