# **Real World Cyber:** Wenn der Cyber-Angriff auf die wirkliche Welt durchschlägt

*„Real World Cyber“* ist keine Fiktion mehr, sondern Realität: Angriffe auf digitale Infrastrukturen beeinträchtigen unser wirkliches Leben. Welche Rolle spielen Länder wie China oder Russland hier? Und: Was müssen wir hierzu wissen, um unsere Infrastrukturen besser vorbereiten und schützen können?

Dror-John Röcher, Geschäftsführer, intcube GmbH

**Achtung, Binsenweisheit:** Wissen ist Macht. Konkret: Das Wissen um die Kronjuwelen der eigenen Organisation und welche IT-Systeme mit ihnen betraut sind, sowie das Wissen um Ziele und Vorgehensweisen von Angreifern. Kennen Cyber-Sicherheitspezialist*innen diese beiden Faktoren, können sie besagte Kronjuwelen erheblich besser und zielgerichteter schützen als Kolleg*innen, denen dieses Wissen – und damit die Macht – fehlt und die somit im Blindflug ans Werk müssen.

Während die meisten Organisationen die Frage nach den Kronjuwelen beantworten können, ist das Wissen um Ziele und Vorgehensweisen von Angreifern deutlich seltener vorhanden. Die Methoden diverser Cyber-Crime-Gruppierungen lassen sich noch halbwegs im Blick behalten, das laufende Beobachten der Angriffsziele und -taktiken staatlicher Akteure jedoch ist eine zeitfressende Spezialdisziplin.

Anhand der Beispiele China und Russland lässt sich sehr gut erläutern, was es rund um die von diesen Nationen ausgewählten strategischen Ziele zu wissen gibt. Die in der Vergangenheit von diesen Akteuren verübten Angriffe, auch auf kritische Infrastrukturen und kritische Sektoren in anderen Ländern, haben weit mehr als nur historischen Wert: Wer die Geschichte kennt, kann daraus ableiten, was die Aktionen beispielsweise für westeuropäische Staaten, deren Wirtschaft und Gesellschaft sowie die Betreiber*innen kritischer Infrastrukturen bedeuten.

# Von schwarzen Schwänen und mächtigen Gegnern



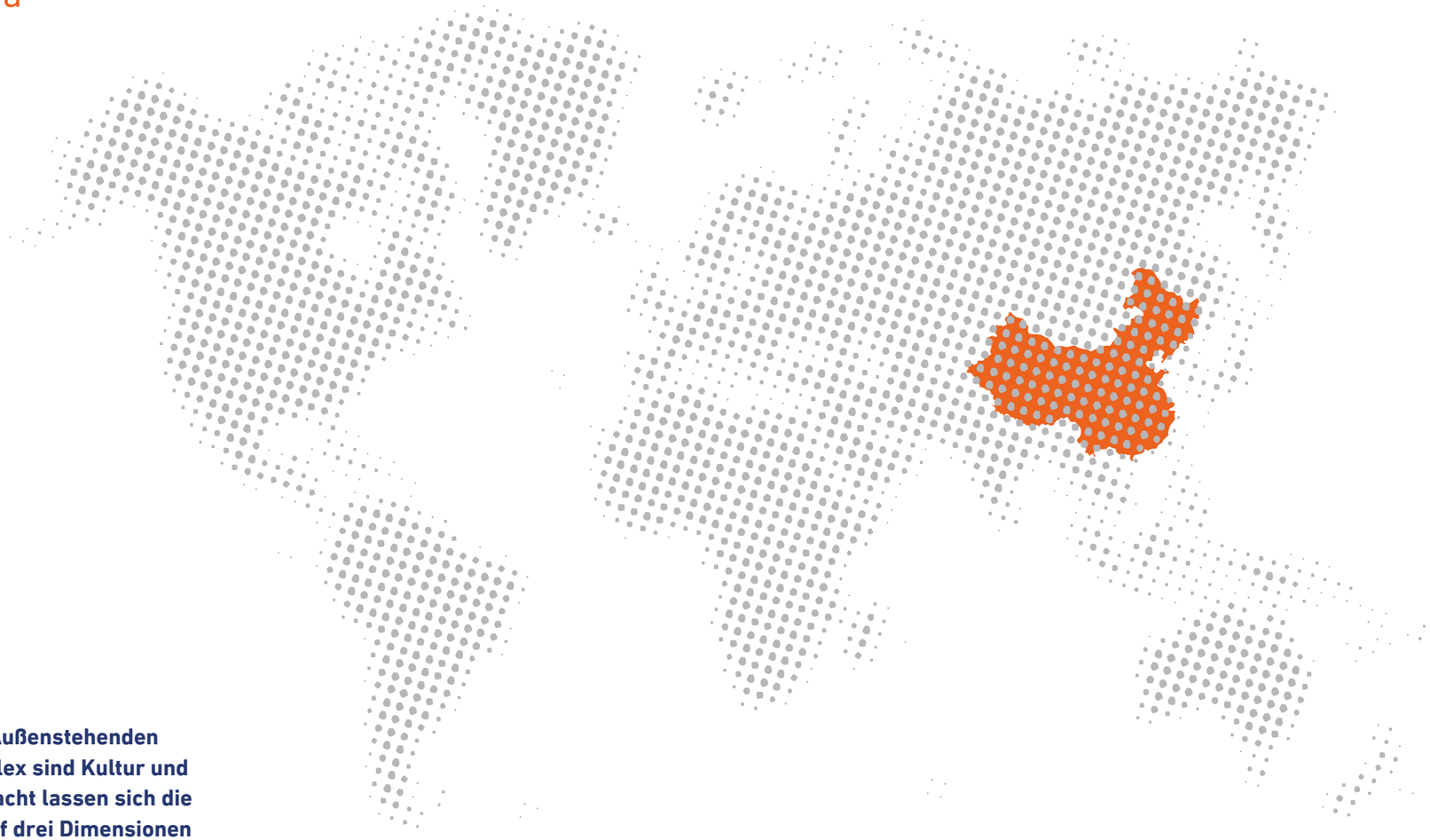
**Die derzeitige Weltlage ist einmalig.** Das Zusammentreffen von gleich fünf sogenannten schwarzen Schwänen – also zuvor vollkommen unwahrscheinlich erscheinenden Ereignissen, die gänzlich überraschend eintreten – gab es so noch nicht. Mit den schwarzen Schwänen sind die Covid-Pandemie, die damit zusammenhängenden Lieferkettenprobleme, der Krieg in der Ukraine, die Inflation sowie die Energiekrise gemeint. Obwohl Klimakrise und demographische Entwicklung ebenfalls relevante, von uns kaum noch veränderbare langfristige Trends sind, sollen diese im Folgenden außen vor bleiben. Die Lage ist komplex genug.

Aufs engste mit den schwarzen Schwänen verbunden sind China und Russland. Die Aktionen des letzteren Landes führen zu akuten Problemen: Die durch den Angriffskrieg auf die Ukraine ausgelöste Energiekriese und damit einhergehende Inflation wirken sich unmittelbar aus. Sie haben zudem das Potential, die Weltwirtschaft nachhaltig für die nächsten drei bis fünf Jahre zu stören. Langfristig dürfte sich das Land auf dem absteigenden Ast befinden.

Die mit China verbundenen Herausforderungen sind eher strategischer als kurzfristiger Natur: Chinas hat eine dominante Position als Werkbank für den Rest der Welt, als Zulieferer, es definiert Standards, ist wichtiger Kreditgeber für afrikanische Staaten, Rohstofflieferant für diverse Länder und sehr wichtig als Käufer von Technologien. Kurzum: Die Welt ist massiv abhängig von China. Gleichzeitig teilen westliche Staaten kein Wertesystem mit China.

Beiden Ländern gemeinsam ist, dass ihnen die westlichen Menschen- und Grundrechte (Meinungsfreiheit, Pressefreiheit und so weiter) nicht wichtig sind. Beide sind autokratisch geführt und haben einen nationalistisch motivierten Großmachtanspruch.

# (Cyber)Weltmacht im Osten: China



**China erschließt sich Außenstehenden selten sofort, zu komplex sind Kultur und Staatssystem. Vereinfacht lassen sich die Ziele der Regierung auf drei Dimensionen herunterbrechen:**

1. Inner-Chinesischer Zusammenhalt, Einheit Chinas und Macht erhalt. Die Regie rung sieht dieses Ziel von der Demokratie-bewegung in Hong Kong sowie einem unab hängigen Taiwan und den Unabhängigkeits-bestrebungen Tibets bedroht.

2. Die regionale Machtprojektion ins Süd-chinesische Meer.

3. Gestaltung der wirtschaftlichen und tech-nologischen Entwicklung mit dem Ziel, im Jahr 2049 – zum 100. Gründungsgeburtstag Chinas – die weltweit führende Nation zu sein.

   Als strategischer Entwicklungspfad dorthin gelten die Fünfjahrespläne.

# (Cyber)Weltmacht im Osten: China

Die Fünfjahrespläne ergeben eine kontinuierliche Weiterentwicklung Chinas. Dabei sind sie nicht länger als Dogma zu verstehen. Vielmehr definieren sie strategische Ziele, die dann in regionalen oder sektoralen Plänen umgesetzt werden. Somit funktionieren sie eher als Kompass und Kontrollinstrument und haben wenig mit den kommunistischen Fünfjahres-Produktionsplänen der Sowjetunion oder der DDR zu tun.

Der bis 2015 gültige Plan beispielsweise hatte die Transformation der Wirtschaft zum Ziel: Ausländische Investitionen in China sollten gefördert werden, der Ausbau von Kern- und Wasserkraft sollte die Stromversorgung stabilisieren und Hochgeschwindigkeitsstrecken für Bahnen sowie Autobahnen Distanzen verkleinern. Der darauffolgende Plan sollte den Grundstein legen für „Made in China 2025". Zu den Zielen gehören ein Upgrade der Industrie, um einen größeren Anteil an den globalen Lieferketten abbilden zu können oder ein besseres Umsetzen von Forschungsergebnissen in der Wirtschaft.

Dem Staat und der kommunistischen Partei Chinas sind alle Mittel recht, um diese Ziele zu erreichen. Insbesondere im Bereich der wirtschaftlichen und technologischen Entwicklung gehören traditionelle Industriespionage und auch Industriespionage mit Cyber-Methoden zum Alltag. Es ist gang und gäbe, dass ausländische Unternehmen, die in einem vom jeweiligen Fünfjahresplan behandelten Sektor aktiv sind, verstärkt attackiert werden. Die klassische nachrichtendienstliche Aufklärung, massiv unterstützt durch Cyber-Methoden,  kommt insbesondere bei den Anrainerstaaten im südchinesischen Meer zur Anwendung.

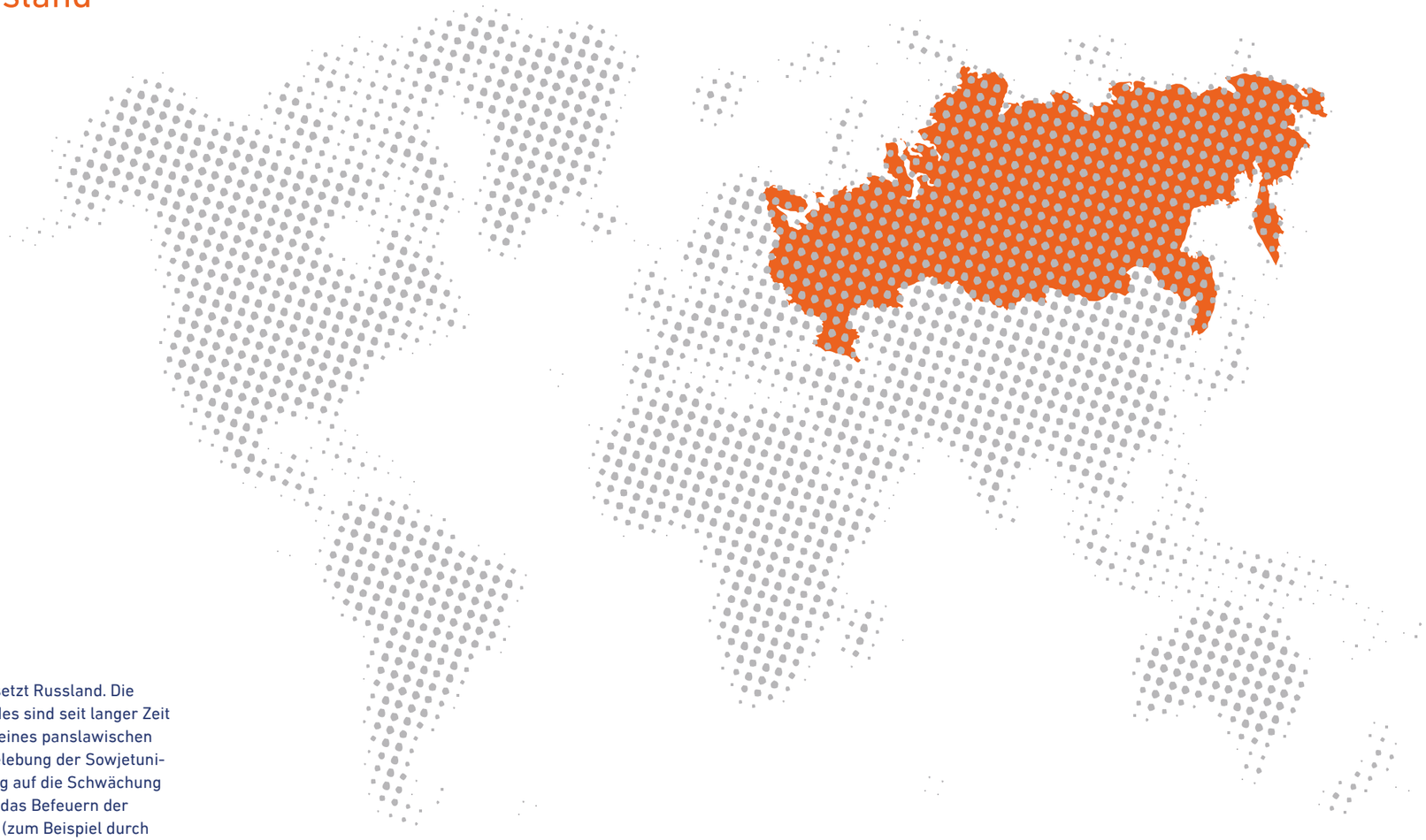
Traditionell verantwortlich für die Informationsbeschaffung war die chinesische Armee (PLA). In den letzten Jahren verlagerte sich die Verantwortlichkeit zum Ministerium für Staatssicherheit. Geändert hat sich auch das Vorgehen. Während die Wirtschaftsspione früher alles an Daten in den ausgeforschten Netzwerken einsammelten, was sie finden konnten, gehen sie heute deutlich leiser, zielgerichteter und langfristiger vor.

Dass China für Spionage und Wirtschaftsspionage offensive Cyber-Aktivitäten startet, ist inzwischen hinreichend belegt. Die wirkmächtigen Supply-Chain-Angriffe, also Attacken, bei denen das eigentliche Ziel durch eine vorhergehende Attacke auf einen Zulieferer ins Visier genommen wird, sind seit dem Jahr 2011 bekannt. So spionierte China beispielsweise den US-Rüstungskonzern Lockheed Martin erfolgreich aus, in dem die staatlichen Cyber-Akteure zuvor den IT-Sicherheitshersteller RSA attackierten. Lockheed Martin nutzte RSA-Produkte, beispielsweise zum Absichern von VPN-Zugängen.

Ein weiteres Beispiel ist eine Reihe von erfolgreichen Angriffen gegen die chemische Industrie Deutschlands in den Jahren 2014 bis 2019. Da die Angriffe auf dieselbe Branche zielten und sehr ähnliche Werkzeuge sowie Methoden zum Einsatz kamen, können sie als zusammengehörende Kampagne begriffen werden. Die als Winnti-Gruppe bekannten Angreifer agierten mindestens teilweise im staatlichen, chinesischen Auftrag und zielten vor allem auf den Diebstahl von Industriegeheimnissen. Dies lag zum Angriffszeitpunkt auf Linie mit dem damaligen *„Made in China 2025"*- Fünfjahresplan.

Sabotage-Akte sind keine typisch chinesische Methode. Allerdings haben staatliche chinesische Hacker in den Jahren 2011 bis 2013 erfolgreich rund zwei Dutzend US-amerikanische Pipelinebetreiber kompromittiert. Die US-Regierung machte dies erst im Juli 2021 nach dem Ransomware-Angriff auf die Colonial Pipeline bekannt.  Hintergrund könnte sein – dies ist allenfalls eine Vermutung –, dass sich China Anfang der 2010er Jahre den Zugriff auf kritische Infrastrukturen in den USA für die Zukunft sichern wollte.

# Land mit Großmacht-anspruch: Russland



Deutlich stärker auf Sabotage setzt Russland. Die strategischen Ziele dieses Landes sind seit langer Zeit bekannt: Neben dem Errichten eines panslawischen Großreichs, quasi der Wiederbelebung der Sowjetunion, zielt die russische Regierung auf die Schwächung Europas (unter anderem durch das Befeuern der Brexit-Bewegung) und der USA (zum Beispiel durch das Spalten der US-Gesellschaft).

Auf staatlicher Seite kümmern sich hauptsächlich drei Dienste um Cyber-Aktivitäten (zu denen auch destruktive Angriffe gehören): der Inlandsgeheimdienst FSB (Föderaler Dienst für Sicherheit der Russischen Föderation; Nachfolger des KGB und Putins „Heimat“), der Militärische Nachrichtendienst GRU (Hauptverwaltung für Aufklärung) sowie der Auslandsnachrichtendienst SVR. Die Dienste stehen teilweise im Wettbewerb zueinander.

Zu den auffälligsten Aktionen des SVR zählen beispielsweise die Supply-Chain-Attacke auf SolarWinds im Jahr 2020 oder der Diebstahl von Industriegeheimnissen rund um Covid-Impfstoffe. Der FSB trat in Deutschland durch Attacken auf das Auswärtige Amt beziehungsweise die Hochschule des Bundes in Aktion. Auf das Konto des GRU gehen beispielsweise die Angriffe auf die Stromversorgung der Ukraine im Jahr 2015, Manipulationen rund um die französische Präsidentschaftswahl im Jahr 2017 oder die destruktive Malware NotPetya, die im Jahr 2017 weltweit Festplatten in Organisationen unwiederbringlich formatiert hat.

Dazu kommt eine Vielzahl krimineller Vereinigungen, die weitgehend straffrei agieren können, solange sie außerhalb Russlands (insbesondere im Westen) aktiv sind. Anders ist auch schwerlich zu erklären, dass im Jahr 2021 zirka 75 Prozent des weltweiten Umsatzes mit Ransomware in Russland landete. Mitunter heuert der russische Staat die Hacker des organisierten Verbrechens auch direkt an.

Zu den Besonderheiten beim russischen Cyber-Vorgehen gehört, dass sich Spionage und Aufklärung auf den militärischen und politischen Bereich konzentriert. Klassische Wirtschaftsspionage ist weniger prominent.  Berüchtigt ist das Land auch für die Manipulation von Meinungen in anderen Ländern durch das Verbreiten von Fake News, seine Troll-Armeen sowie die verdeckte Unterstützung von Vereinen, Gruppen, Parteien und Think Tanks im Ausland. Außerdem scheuen sich die russischen Dienste nicht, destruktive Malware einzusetzen. Allen voran sogenannte Wiper wie NotPetya, das eigentlich auf ukrainische Organisationen zielte, dann aber außer Kontrolle geriet und weltweit erhebliche Schäden anrichtete.

# Cyber im Krieg: Der Angriff Russlands auf die Ukraine

Wie der Zeitpunkt von NotPetya vermuten lässt, begann der Ukraine-Krieg nicht erst am 24. Februar 2022 sondern schon im Jahr 2014 mit der Besetzung der Krim und den Kämpfen in der Ostukraine. Und auch die Cyber-Domäne spielt von Anfang an eine signifikante Rolle.

Die offensiven Cyber-Angriffe gegen die Ukraine beginnen ungefähr im Sommer 2013. Seitdem startete Russland viele und regelmäßige Kampagnen. Ungefähr die Hälfte der Angriffe richtete sich gegen die ukrainische Regierung, ihre Behörden und Mitarbeiter*innen. An zweiter Stelle rangieren Attacken auf kritische Infrastrukturen – insbesondere die Stromversorgung geriet immer wieder ins Visier.

Durch solche Angriffe auf kritische Infrastrukturen wie Strom, Telekommunikation oder Logistik wird einerseits Terror in der Bevölkerung erzeugt, das Vertrauen in die eigene Regierung und Verwaltung unterminiert und andererseits werden die operativen Fähigkeiten des Gegners beeinträchtigt. Letzteres kann ein Aggressor insbesondere begleitend zu anderen Aktivitäten einsetzen, um ihre Wirkung zu verstärken.

Zu Beginn des Angriffskrieges im Februar 2022 erwarteten etliche Fachleute einen „Cybergeddon", also verheerende Cyber-Attacken durch Russland, die begleitend zu den regulären, kinetischen Angriffen stattfinden. Es gab in der Tat auch einige Vorfälle, die bekannt wurden. Von anderen werden wir eventuell erst in Zukunft erfahren. So attackierte Russland gezielt Telekommunikationsinfrastruktur, um die Koordinations- und Reaktionsfähigkeit des ukrainischen Militärs einzuschränken.

Wie der Hack der Modems, die für die Kommunikation mit dem Satellitennetzwerks von Viasat verantwortlich sind, am ersten Kriegstag belegt, können Cyberangriffe völlig ungeahnte Kollateraleffekte nach sich ziehen – viel mehr noch als physische Angriffe. So fielen durch den Angriff nicht nur die Modems in der Ukraine aus. Es waren darüber hinaus auch gut 6000 Modems in Deutschland betroffen, die zur Fernwartung von Windkraftanlagen dienen. Der Cyberangriff war also gleich in zweierlei Hinsicht grenzüberschreitend: Es gerieten Modems außerhalb des Kriegsgebiets unter die Räder und die Wirkung beschränkte sich nicht auf den Cyber-Raum, sondern erstreckte sich bis in die reale Welt.

Unterm Strich sieht es derzeit so aus, als hätten die Cyberangriffe während des Krieges geringere Auswirkungen, als Russland sich dies erhofft haben dürfte. Der „Cybergeddon" blieb bislang zum Glück aus. Verlassen sollte man sich künftig auf einen solch glimpflichen Ausgang aber nicht.

Seitdem die russische Armee in der Defensive ist, verlagert Russland vermutlich seine Cyber-Aktivitäten weg von der offensiven Unterstützung hin zu klassischer militärischer Aufklärung. Dies geschieht parallel zum Wandel vom hybriden, irregulären Krieg hin zum regulären Stellungskrieg.

Hinzu kommt, dass die russischen Angreifer etliche ihrer gehackten Zugänge in die ukrainischen Netze, die sie sich über die letzten Jahre erarbeitet haben, durch das andauernde Nutzen verbrannt haben dürften. Das Schaffen neuer Zugänge ist mühselig und zeitraubend und vermutlich derzeit nicht oberste Priorität der russischen Staatshacker. Und die Ukrainer, die sich seit 2013 in einer andauernden, aktiven Cyber-Defensivlage befinden und dabei auch signifikante Unterstützung der US-amerikanischen Nachrichtendienste erhalten, sind aufgrund der Dauerübung bestens aufgestellt und gerüstet, um den russischen Cyberangriffen entgegenzutreten.

Es ist bekannt, dass die USA der Ukraine auch beim sogenannten „Threat-Hunting" halfen, also der aktiven Suche nach Auffälligkeiten in ukrainischen Netzen. Da Russland die Ukraine seit vielen Jahren als Testlabor für ihre Cyber-Angriffswerkzeuge nutzen, können Threat-Hunter in den ukrainischen Netzen die Methoden und Werkzeuge der russischen Angreifer studieren und mit den damit gewonnen Erkenntnissen die Detektionsfähigkeiten verbessern. Die USA haben sich auch dazu bekannt, die Ukraine in gewissem Umfang mit offensiven Cyberaktivitäten zu unterstützen. Auch wenn unbekannt ist, was genau damit gemeint ist, dürfte es sich um sogenannte „forward hunting"-Aktivitäten handeln, die knapp unterhalb einer direkten Aggressionsschwelle liegen. Diese Aktivitäten zielen vermutlich darauf ab, Schwachstellen in russischen Systemen zu identifizieren, die für die konventionelle und digitale Kriegsführung verwendet werden.

Neben diesen Aktivitäten staatlicher Akteure gibt es auch ein Echo des Krieges bei politisch motivierten Hackergruppen, den sogenannten Hacktivisten. Diese Gruppen, die auf beiden Seiten aktiv sind, versuchen – mehr oder weniger erfolgreich – vom heimischen PC aus in das Geschehen einzugreifen oder das öffentliche Meinungsbild zu beeinflussen. Zu den typischen Methoden zählen DDoS (Distributed Denial of Service)- Angriffe, also Attacken, die auf eine Überlastung von Systemen und Kommunikationsleitungen abzielen, die Manipulation von Webseiten-Inhalten, um politische Botschaften zu verbreiten, sowie – in geringerem Umfang – das Veröffentlichen gestohlener Daten auf speziellen Leak-Seiten. Auch wenn die Effekte dieser Hacktivisten im Gesamtkontext eher gering sind, so können die einzelnen Aktionen betroffenen Unternehmen und Organisation massiven Schaden zufügen.

# Cyber muss immer mit in den Fokus

Angesichts der vielen kinetischen Angriffe auf kritische Infrastruktur während des Krieges, wird klar, dass solche Angriffe in aktiven Kriegssituationen oft einfacher umzusetzen sind als komplexe Cyber-Operationen.

Gleichzeitig belegen die beobachteten Cyber-Angriffe, dass *„Real World Cyber"*, also das Überschwappen von Cyber-Angriffen in die wirkliche Welt, keine Fiktion mehr ist. Der Cyber-Raum ist inzwischen eine weitere Dimension, in der Staaten, aber auch Organisationen ihre eigenen Interessen vertreten und verteidigen. Nicht nur China und Russland verfolgen ihre strategischen Ziele auch im Cyberraum, sondern auch viele andere Staaten wie Iran, Israel, Nordkorea oder die USA. Daher müssen Cyber-Angriffe in all unsere strategischen und taktischen Überlegungen mit einbezogen werden. Damit wir uns besservorbereiten können.

Durch Verständnis der Aktivitäten im Cyberraum, die eben auch in der Konfliktphase unterhalb des Krieges stattfinden, kann man auch auf die Motivationslage von Akteuren schließen. Wir können diese Erkenntnis nutzen, um uns vorzubereiten. Im offenen Krieg und wenn Zerstörung das Ziel ist, sind kinetische Angriffe weiterhin effektiver.

Aber im kalten Krieg, auf den wir sowohl mit Russland als auch mit China zusteuern, wird Cyber auch in Zukunft eine immens wichtige Rolle spielen – vielleicht sogar noch mehr als heute, da mit vergleichsweise geringem Mitteleinsatz und Risiko signifikante Erfolge erzielbar sind.

Und was bedeutet all dies für Organisationen, die nicht unmittelbar am Krieg beteiligt sind oder zufällig zum Kollateralschaden werden? Eine der Lehren sollte sein, dass staatliche Akteure eine Vielzahl an Zielen auf jeweils unterschiedlichen Wegen verfolgen. Und dass man sich nur dann effektiv und passgenau schützen kann, wenn man Ziele und Wege kennt. Generell ist Westeuropa in dieser Hinsicht bislang zu naiv und strukturell schlecht aufgestellt. Dies wird durch die beispiellose Verantwortungsdiffusion in der deutschen Cyber-Sicherheitsarchitektur überdeutlich.

Neben strukturellen Reformen, die den politischen Willen beinhalten müssen, alte Zöpfe abzuschneiden und wohldotierte Posten und Abteilungen abzulösen, ist auch ein Umdenken bei Unternehmenslenkern und Entscheidern notwendig. Neben der – mittlerweile akzeptierten – Realität des digitalen Verbrechens, die sich seit Jahren in immer neuen Ransomware-Vorfällen widerspiegelt, muss auch die Realität der staatlich gelenkten Cyber-Angriffe, Spionage, Sabotage und Meinungsmanipulation akzeptiert werden. Erst mit dieser Akzeptanz ist ein Umdenken und Handeln möglich.

Unabdingbar ist auch, dass wir das Wissen um die Angreifer, ihre Ziele und Methoden kontinuierlich aktualisieren müssen. Diese Aufgabe, die früher exklusiv den Nachrichtendiensten zukam, muss auch in der Wirtschaft angegangen werden.

Nachdem kaum eine Organisation die personellen Ressourcen hat, um eine fortlaufende Recherche selbst zu erledigen, empfiehlt sich der Zusammenschluss zum Verbund sowie der zielgerichtete Einkauf von externer Expertise. In der Hoffnung, dass die auf Basis des eingebrachten Wissens verbesserten Schutzmaßnahmen dafür sorgen, dass die eigene Organisation kein *„Real World Cyber"*-Erlebnis erfährt.

# **25 Years of** Cyber Security Experience

## Q & A



**Kontakt:**
https://linkedin.com/in/droecher

**Whitepaper:**
https://intcube.io/publications


intcube.io