WWW.OEAW.AC.AT

ÖAW ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN

**MONTAG, 16. SEPTEMBER 2019**
**BEGINN: 18.00 UHR**
**ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN**
**FESTSAAL**
**DR. IGNAZ SEIPEL-PLATZ 2, 1010 WIEN**

© Shutterstock

**PODIUMSDISKUSSION**

# BLACKOUT DURCH CYBERWAR

## FIKTION ODER REALITÄT?

# PROGRAMM

## BEGRÜSSUNG UND EINLEITUNG

**Georg Brasseur** | Präsident der mathematisch-naturwissenschaftlichen Klasse der Österreichischen Akademie der Wissenschaften

## PODIUMSDISKUSSION

*Blackout durch Cyberwar: Fiktion oder Realität?*

**Carina Kloibhofer** | Research Engineer
Center for Digital Safety & Security, Austrian Institute of Technology GmbH (AIT)
**Dietmar Mandl** | Chief Information Security Officer and Data Protection Officer, Austrian Power Grid (APG)
**August Reinisch** | Professor für Völker- und Europarecht
Institut für Europarecht, Internationales Recht und Rechtsvergleichung, Universität Wien
Korrespondierendes Mitglied der Österreichischen Akademie der Wissenschaften
**Walter Unger** | Leiter der Abteilung „Cyber Defence“
Bundesministerium für Landesverteidigung (BMLV)

**Moderation:**
**Thomas Eiter** | Professor für Wissensbasierte Systeme
Institut für Informationssysteme, Technische Universität Wien
Korrespondierendes Mitglied der Österreichischen Akademie der Wissenschaften

Im Anschluss an die Veranstaltung wird zum Empfang in die Aula geladen.

**ANMELDUNG** bis 12. September 2019 erbeten:
*www.oeaw.ac.at/anmeldung/blackout-durch-cyberwar-fiktion-oder-realitaet/*

**KONTAKT:** Julia Weilinger, BA, Österreichische Akademie der Wissenschaften
T: +43 1 51581-1214, julia.weilinger@oeaw.ac.at

## BLACKOUT DURCH CYBERWAR: FIKTION ODER REALITÄT?

Waren elektrische Effekte vor knapp mehr als zweihundert Jahren noch eine Kuriosität, die bei Vorführungen in herrschaftlichen Salons bestaunt wurde, so hat die weitere Erforschung der Elektrizität zur Entwicklung einer Technologie geführt, die heute für die Menschheit von zentraler Bedeutung ist. Ohne elektrischen Strom geht in der modernen Welt so gut wie gar nichts mehr, Wirtschaft und Gesellschaft sind stark von ihm abhängig. Ein länger andauernder, flächendeckender Stromausfall kann, wie Beispiele aus der Vergangenheit zeigen, schwerwiegende Folgen haben.

Die Stromversorgung zählt somit zur kritischen Infrastruktur eines Landes, deren Funktionstüchtigkeit essentiell ist. Längst gehören störende Eingriffe in sie zu erklärten Maßnahmen, um ein Land gezielt in Versorgungsprobleme zu stürzen und damit eine Destabilisierung oder gar den Zusammenbruch herbeizuführen. Mit der wachsenden Vernetzung von Computersystemen und der zunehmenden Digitalisierung sowie Fortschritten bei der künstlichen Intelligenz ergeben sich zudem Möglichkeiten, auf Software-Ebene Angriffe auf die kritische Infrastruktur vorzunehmen. Letztere werden oft als mögliche Aktionen in einem Cyberwar genannt, der zwischen Konfliktparteien entbrennt und im Stillen geführt wird.

Es stellt sich die Frage, ob die Lahmlegung der Stromversorgung durch Aktionen im Rahmen eines Cyberwars eine reale Bedrohung darstellt oder, vom Stand der Technik betrachtet, nur Fiktion ist. Diese Frage soll im Rahmen einer Podiumsdiskussion erörtert werden, in der Expert/inn/en zu Aspekten mehrerer relevanter Themenbereiche zu Wort kommen.
Dazu zählen die Bereiche Hackerangriffe und Cyber-Attacken, vertreten durch Carina Kloibhofer (Austrian Institute of Technology), Energienetze und deren Betrieb, vertreten durch Dietmar Mandl (Austrian Power Grid), Cyber-Abwehr, vertreten durch Walter Unger (Bundesministerium für Landesverteidigung), sowie völkerrechtliche Aspekte, vertreten durch August Reinisch (Universität Wien).

## KURZSTATEMENTS DER TEILNEHMER/INNEN

**Carina Kloibhofer**
*Austrian Institute of Technology*

Betreiber kritischer Infrastrukturen sind denselben Bedrohungsszenarien und Angriffsvektoren ausgesetzt wie jede andere Organisation. Moderne Angriffe erfolgen jedoch meist über längere Zeiträume unbemerkt und können bei erfolgreicher Durchführung gravierende Auswirkungen haben. Am AIT werden AI-basierte Lösungen entwickelt, um derartige Angriffe frühzeitig zu erkennen und größeren Schaden abzuwehren.

**Dietmar Mandl**
*Austrian Power Grid*

Aufgrund des Ausstiegs der österreichischen und europäischen Stromerzeugung aus fossilen Energieträgern und des massiven Ausbaus der erneuerbaren Energiequellen wie Sonne und Wind steht die Energiebranche vor einem gewaltigen Umbruch. Durch die Volatilität der erneuerbaren Energiequellen müssen heutzutage umfassende Maßnahmen zur Sicherstellung der Netzstabilität getroffen werden. Parallel dazu erhöht die Digitalisierung und Elektrifizierung in vielen Lebensbereichen die Komplexität des Gesamtsystems enorm und schafft so potentielle Verwundbarkeiten und neue Angriffsvektoren.

**August Reinisch**
*Universität Wien, Österreichische Akademie der Wissenschaften*

„Cyber incidents", „malicious cyber activities" oder gar der Begriff „cyber warfare" beschäftigen Jurist/inn/en seit einiger Zeit, ohne dass die grundsätzliche rechtliche Frage, ob die Regeln des klassischen Kriegsrechts oder besser des Rechts der bewaffneten Konflikte überhaupt anwendbar sind, gelöst wäre. Die Debatte, ob und wann Cyber-Vorfälle die Schwelle der Anwendung des „Tallinn Manual on the International Law Applicable to Cyber Warfare" überschreiten, bleibt aber ebenso offen wie das rechtspolitische Problem, ob das humanitäre Völkerrecht überhaupt Regelungen vorsieht, die dem innerstaatlichen Recht der Verbrechensbekämpfung (Strafrecht) vorzuziehen sind.

**Walter Unger**
*Bundesministerium für Landesverteidigung*

Cyber Defence ist eine gesamtstaatliche Herausforderung. Cyber-Angriffe gegen die Souveränität eines Staates werden vermutlich gegen die strategischen Infrastrukturen gerichtet sein. Im Sinne der umfassenden Sicherheitsvorsorge sind daher Cyber-Sicherheit, Cyber-Krisenmanagement und Landesverteidigung im Cyber-Raum gesamtstaatlich zu organisieren.

Fotos:
Kloibhofer: © AIT
Mandl: © Mandl
Reinisch: © U. Kriebaum
Unger: © Unger