Future Strategists Hub

Think Europe outside the box

2018

# Handlungsempfehlungen

**Arbeitsgruppe: Digitalisierung und umfassende Sicherheit**

**Leitung: Thomas Lohninger**

# Der Future Strategists Hub

Europa hat eine Vielzahl an strategischen Herausforderungen zu bewältigen. Diese reichen vom Umgang mit Chinas wirtschaftlicher Dynamik über die stagnierende EU-Erweiterung am Westbalkan, und die weitreichenden Entwicklungen der Digitalisierung, die mit vielen Lebensbereiche einhergehen, bis zu sozio-ökonomischen Problemstellungen in West- oder Subsahara-Afrika. Gerade die Folgen der Umbrüche im arabischen Raum werfen oft die Frage auf, wie Europa seine Rolle zwischen Zivilmacht und außen- bzw. sicherheitspolitischem Akteur wahrnehmen soll.

Bis jetzt konnte Europa noch keine überzeugenden Strategien vorlegen, wie man auf diese Palette an Aufgaben reagieren könnte und neue Handlungsspielräume sowie Alternativen der Politik miteinbezieht.

Es braucht daher neue Ideen und zugleich junge Stimmen. Diese frischen Zugänge wurden im Rahmen des Future Strategists Hub diskutiert. Seriöse Ansätze außerhalb des Mainstreams belebten den europäischen Diskurs und identifizierten blinde Flecken.

Der Future Strategists Hub ist ein junges strategisches Format, das Shabka am 07. März 2018 gemeinsam mit dem Institut für Friedenssicherung und Konfliktmanagement (IFK) veranstaltete. Im Future Strategists Hub gestalteten wir Außen-, Sicherheits- und Entwicklungspolitik durch Ideen von talentierten jungen Köpfen, die sich proaktiv bei uns einbrachten. Letztendlich kann eine zukunftsfähige Politik nur zusammen entstehen.

Beim eintägigen Workshop förderten wir in acht thematischen Arbeitsgruppen unter der Leitung je einer Expertin/eines Experten die Erstellung von Politikempfehlungen zu Themen, die Europa bewegen.

Eine Podiumsdiskussion mit den ArbeitsgruppenleiterInnen des Future Strategists Hub rundete den Workshop ab.

Insgesamt arbeitete ein 10-köpfiges Organisationsteam und neun ArbeitsgruppenleiterInnen seit Frühjahr 2017 in enger Zusammenarbeit mit dem IFK an der Vorbereitung des Future Strategists Hub.

Mit dem Future Strategists Hub konnte sich Shabka als junges strategisches Format in Österreich - und dahingehend als strategischer Think&Do-Tank, der auf zivilgesellschaftlicher Basis Akzente und Impulse setzt, etablieren.

Für uns ist Wissen praktisch, sichtbar und umsetzbar. Wir gehen dorthin, wo Ideen gebraucht werden. Das ist unser Verständnis von Ganzheitlichkeit und so verleihen wir unserer Arbeit tatsächliche Wirkkraft.

Unser Credo ist: Verstehen. Entscheiden. Handeln.

## Arbeitsgruppen

- **AG - Zivilgesellschaft im Konflikt**
  **Leitung: Sherin Gharib, Verena Gruber**
- **AG - Digitalisierung und umfassende Sicherheit**
  **Leitung: Thomas Lohninger**
- **AG - Entwicklungspolitik re-loaded**
  **Leitung: Youssouf Simbo Diakite**
- **AG - Europäische Interventionen**
  **Leitung: Johann Wolfschwenger**
- **AG - Stagnierende EU-Annäherung am Westbalkan**
  **Leitung: Adnan Ćerimagić**
- **AG - Strategische Vorausschau für die EU**
  **Leitung: Velina Tchakarova**
- **AG - Wirtschaftsbeziehungen mit Zentralasien**
  **Leitung: Peter Buchas**
- **AG - EU und Menschenrechte**
  **Leitung: Bernadette Knauder**

*Arbeitsgruppe*

# Digitalisierung und umfassende Sicherheit

Durch die Digitalisierung stehen althergebrachten Machtstrukturen vor großen Veränderungen. Noch nie war es so einfach Daten über ganze Bevölkerungsgruppen zu erfassen, auszuwerten und in algorithmischen Entscheidungsprozesse über Individuen miteinzubeziehen. Vernetzte Wirtschaftskreisläufe, Fabriken und Mediensysteme bieten neue Angriffsoberflächen für eine Vielzahl von Akteuren. Gleichzeitig änderte sich die Sicherheitsdoktrin vieler Länder und definiert moderne Bedrohungen zusehends innerhalb der eigenen Bevölkerung. Vor diesen Herausforderungen ist die Netzpolitik zu einem der spannendsten Politikfelder geworden. In ihr wird gleichsam diskutiert ob und wie die Politik regulierend auf das Internet eingreift und wie moderne Technologien die Spielregeln der politischen Bühne neu sortieren.

Militärische Auseinandersetzungen entdecken seit einigen Jahren das Internet als fünfte Domäne (vulgo Cyberwar). Mit dem Sabotageprogramm Stuxnet, das gegen das iranische Atomprogramm eingesetzt wurde, ist der digitale Erstschlag bereits erfolgt. Die erschreckende Verbreitungsrate von Stuxnet über Millionen von Heimrechnern hin zu seinem Ziel in der Urananreicherungsanlage in Natanz ist eine inhärente Bedrohung dieser neuen Waffengattung. Der Erpressungstrojaner Stuxnet infizierte über ein einzelnes Wochenende Millionen von Computersystemen und legte dabei britische Krankenhäuser, spanische Mobilfunknetze und die Deutsche Bahn lahm. Die notwendigen Sicherheitslücken in weit verbreiteten IT-Systemen sind die gemeinsame Voraussetzung dieser neuen Bedrohungen, welcher in Österreich im Rahmen der Legalisierung staatlicher Spionagesoftware (Bundestrojaner) aktuell diskutiert werden.

Eine umfassende Sicherheitsdebatte darf deshalb niemals den Blick auf die Grund- und Freiheitsrechte der Betroffenen und die technischen Realitäten der technischen Systeme verlieren.

## Fragestellungen

- **Was sind die Chancen und Risiken des aktuellen Sicherheitspakets vor dem Hintergrund der Grundrechte aller betroffenen Stakeholder?**
- **Wie kann eine umfassende Sicherheitsdebatte den technischen Realitäten der digitalisierenden Gesellschaft gerecht werden?**
- **Welche Handlungsfelder ergeben sich für die österreichische Außenpolitik durch die wachsende Aufrüstung mit digitalen Angriffswaffen?**

**AG-Leitung: Thomas Lohninger**

ist Geschäftsführer des Arbeitskreis Vorratsdaten Österreich. Er hat für European Digital Rights als Policy Advisor an den Netzneutralitäts-Aspekten der Telekom Binnenmarkt Verordnung gearbeitet.

Er arbeitete 8 Jahre lang als Programmierer und Systemadministrator, hat einen Bachelor in Kultur- und Sozialanthropologie und arbeitet seit 2012 als Trainer für praktische IT-Sicherheit. In seiner Freizeit produziert er Podcasts im Bereich Wissenschaft und Technik.

*AG Digitalisierung und umfassende Sicherheit*

# Handlungsempfehlungen

## IT-Sicherheit in der Privatwirtschaft

- **Anreize für mehr IT-Sicherheit in der Privatwirtschaft**
  Finanzielle Anreize für große Unternehmen über 500 Mitarbeitern und Haftungen für die Leitungsebene bei multinationalen oder staatsnahen Unternehmen zur Umsetzung von Mindeststandards für IT-Sicherheitsmaßnahmen. Diese Sicherheitsmaßnahmen sollen über ISO-Normen (zB ISO27000) oder Gremien aus Wirtschaft, Wissenschaft und Zivilgesellschaft erstellt werden. (Standortvorteil für Österreich, wenn unsere Unternehmen besonders auf IT-Sicherheit achten)
- **Transparentes Ablaufdatum für Sicherheitsupdates**
  Beim Kauf von elektronischen Geräten mit Netzwerkfunktionalität muss dem Konsumenten ein Mindestablaufdatum für Sicherheitsupdates genannt werden. Der Gerätehersteller verpflichtet sich, mindestens bis zu diesem Datum Sicherheitsupdates für dieses Gerät in seiner default Konfiguration zu liefern.
- **Förderprogramme für Maßnahmen zur Steigerung von IT-Sicherheit in kleinen und mittleren Unternehmen**
- **Aufstockung der Ressourcen der Datenschutzbehörde**

## Schutz der nationalen Sicherheit vor digitalen Angriffen

- **Internationale Abrüstungsabkommen für Cyberwaffen**
  Bundestrojaner und andere staatlich geduldete Schadsoftware und Cyberangrifswaffen gefährden die nationale Sicherheit Österreichs auf einer noch nie da gewesenen Ebene. Österreich wird sich am Rüstungswettlauf in der fünften Domäne (vulgo Cyberspace) nicht beteiligen. Die Vorteile für Strafverfolgungsbehörden durch die Überwachung von Zielpersonen mit einem Bundestrojaner stehen in keinem Verhältnis zu den Gefahren für die Geräte unseres alltäglichen Gebrauchs und unserer kritischen Infrastruktur. Dermaßen gewonnen Beweise sind durch die Infektion und Fernsteuerung des Zielgeräts in rechtsstaatlichen Gerichtsverfahren nicht verwertbar. Österreich muss hier Vorreiter sein und deshalb setzt sich die Bundesregierung künftig für ein internationales Abrüstungsabkommen für digitale Angriffswaffen ein.
- **Schutz der Bevölkerung vor digitalen Angriffswaffen**
  Schutz unserer Netze vor Angriffen durch Fokussierung auf Verteidigungskapazitäten im staatlichen Bereich. Der Einsatz digitaler Angriffswaffen gegen zivile Einrichtungen muss zu Sanktionen auf diplomatischer Ebene führen.
- **Verantwortungsvoller Umgang mit Sicherheitslücken**
  Etablierung staatlich finanzierter Bug-Bounty-Programme zur Steigerung des Anreizes von Responsible Disclosure. Sicherheitslücken müssen in einer angemessenen Frist veröffentlicht werden.

## Förderung europäischer Digitalwirtschaft

- **Österreich muss die Schweiz der Datensicherheit werden**
  Standortvorteil für Österreich durch Positionierung als innovativer Safe Harbour der Datensicherheit. Als Schweiz der Datensicherheit sind wir besonders attraktiv für Betriebansiedlungen, z.B. zum Schutz ihrer besonders sensiblen Daten. Durch den starken Fokus auf Wasserkraft ist Österreich besonders gut geeignet für Datenzentren unter ökologischen Bedingungen. Keine Firma kann es sich leisten, wenn ihre IT für mehrere Stunden still steht. Österreich bietet höchste Stabilität und Sicherheit.

- **Unabhängige Behörde für die IT-Sicherheit**
  Trennung von anderen Stellen, die für die Unterwanderung von IT-Sicherheit zuständig sind (BSI in Deutschland, BVT in Österreich). Diese Behörde soll Informationsmaterialien und Beratungsleistungen anbieten, sowie technische Gutachten und Empfehlungen erlassen und als Anlaufstelle in IT-Sicherheitsfragen für KMUs, WhistleBlower und die Berufsvertretungen dienen.
- **Investitionsprogramme für europäische Digitalwirtschaft**
  Über eine hohe Besteuerung von online Werbung sollen datenschutzfreundliche Geschäftsmodelle europäischer Firmen gefördert werden. Kriterium für den Erhalt dieser Förderungen ist ein europäischer Eigentumsvorbehalt, der einen Ausverkauf dieser Unternehmen für die nächsten 30 Jahre verbietet.
- **Interoperabilität und Datenportabilität für dominante soziale Netzwerke**
  Nutzer müssen zu ihrem Recht unter DSGVO kommen ihre Daten von sozialen Netzwerken exportieren und zu Konkurrenten importieren zu können. Soziale Netzwerke über einer gewissen Größe müssen die Kernfunktionalitäten für ihre Konkurrenten öffnen, sodass Nutzer nicht auf Facebook sein müssen, um mit ihren Freunden dort in Kontakt zu bleiben.

## Bildung

- **Steigerung von Medienkompetenz horizontal im gesamten Bildungssystem, sowohl bei Lehrmaterialien als auch im Bezug auf modernisierte Lerninhalte.**
- **Datenschutz und IT-Sicherheit in die Ausbildung von technischen Berufen integrieren (HTL, Fachhochschule, TU)**
- **Offenes Schulbuch**
  Didaktisch gut aufgearbeitete Lehr- und Schulungsmaterialien unter freier Lizenz in editierbarer Form im Internet (Wiki).
  Bsp: Demokratiewerkstatt, Sexualaufklärung, Sprachtrainings im Flüchtlingsbereich

# Informationen

## Teilnehmer

- **AG-Leitung: Thomas Lohninger**
- Lena Pieber
- Florian Müllner
- Sebyll Ildiko Onbasi
- Julia Litofcenko
- Thiago Carneiro
- Daniela Platsch
- Verena Hanna
- Basma Salama
- Nikolaus Brandstetter

## Kontakt

presse-fsh@shabka.org
office-fsh@shabka.org

www.shabka.org
fsh.shabka.org
office@shabka.org
www.facebook.com/shabka.infonet
twitter.com/shabka_infonet
www.youtube.com/user/ShabkaInfoNet
vimeo.com/shabka

## Impressum:

Für den Inhalt verantwortlich:

Shabka - Network for a Global Society, www.shabka.org, office@shabka.org, ZVR: 718036080

Layout:

Thomas König, Lukas Wank