Cyber Diplomacy - neue Technologien in der Diplomatie

Autoren: Carolin Klimt, Laurent Piazzi, Paula Raffaseder, Leonora Vrankulj, Philip Tudor

Im Zeitalter der digitalen Technologien hat sich die Art und Weise der zwischenstaatlichen Interaktion maßgeblich verändert. Die traditionelle Diplomatie durchläuft eine Transformation, die durch den Einbezug digitaler Mittel und die Entstehung neuer Herausforderungen, aber auch neuer Chancen geprägt ist. Dabei gliedert sich dieses Thema in folgende Bereiche: Die Arten der Diplomatie, gezielte Desinformation, Cyber-Attacken sowie der Einfluss von Technologieunternehmen auf diplomatische Prozesse.

Definition
Um den Begriff der Cyber Diplomacy besser verständlich zu machen, wird in diesem Papier zwischen drei verschiedenen Kategorien unterschieden. Diese Bezeichnungen werden im allgemeinen Sprachgebrauch sehr oft verwechselt, beschäftigen sich jedoch mit verschiedenen Problematiken. In der Praxis fallen verschiedene Themen in mehrere Bereiche. Aus diesem Grund sind Angelegenheiten der Cyber Diplomacy nicht ausschließlich aus einer dieser Perspektiven zu betrachten. Vielmehr wird es durch die Ergänzung aller Bereiche möglich, ein komplexes Thema besser zu verstehen.

Der Aspekt der **Cyber Diplomatie** befasst sich mit dem Einsatz von diplomatischen Werkzeugen für die Stärkung der internationalen Cyber Security. Das Bekämpfen von Cyber-Kriminalität fällt in diesen Aufgabenbereich. Um dies effektiv durchführen zu können, besteht der Fokus auf das Entwickeln von international harmonisierenden Normen und Regeln. Diese sollten Angriffe auf wichtige Infrastrukturen vorbeugen und die Länder auf einen gemeinsamen Standard befördern.

Die Beziehungen zwischen Staat und großen Unternehmen haben in letzter Zeit an massiver Wichtigkeit gewonnen. Vor allem durch Innovationen im Bereich der künstlichen Intelligenz müssen Rahmenbedingungen für einen sicheren und verantwortungsbewussten Umgang mit der neuen Technologie definiert werden. Die **Technologie Diplomatie** setzt sich mit der Regulierung von derartigen Entwicklungen auseinander und versucht durch Gesetze wie dem Digital Service Act oder dem AI-Act eine nachhaltige Entfaltung zu motivieren.

Die **Digitale Diplomatie** hebt die Wichtigkeit von digitaler Kommunikation hervor. Soziale Medien sind ein essenzieller Bestandteil der Gesellschaft und müssen bei der Weiterentwicklung von diplomatischen Vorgängen unbedingt berücksichtigt werden. Allerdings beschränkt sich dieser Bereich nicht nur auf das Auftreten auf den verschiedenen Kanälen. Das Vorbereiten von virtuellen Veranstaltungen zur Informationsweitergabe und zur Erleichterung der Zugänglichkeit dieser ist ebenso ein Bestandteil. Aus diesem Grund fällt auch das Weiterentwickeln von diversen Online-Diensten unter diesen Punkt. Ausreichendes Verständnis digitaler Diplomatie ermöglicht es einem Staat, auf eine effiziente Art und Weise Informationen zu teilen und das nationale sowie internationale Notfall- und Krisenmanagement zu verbessern.

Desinformation
Desinformation wird definiert als die gezielte Verbreitung falscher Informationen mit dem Ziel, öffentliche Meinungen zu manipulieren, Missverständnisse zu fördern und politische, wirtschaftliche und soziale Ziele zu erreichen.

Ein typisches Beispiel sind die Deepfakes, bei denen mithilfe von künstlicher Intelligenz (KI) täuschend echte Fotos oder Videos generiert werden. Diese werden dann mit dem Ziel der politischen Destabilisierung verwendet, indem sie Politiker in heiklen Situationen zeigen, gesellschaftliche Spaltungen vertiefen, politische Gegner schwächen oder Wahlen beeinflussen. Zudem können Deepfakes diplomatische Beziehungen schwächen, indem sie Missvertrauen zwischen Staaten bilden.

Gegenmaßnahmen umfassen die Kennzeichnung KI generierter Inhalte, den Einsatz von Algorithmen zur Erkennung von Deepfakes sowie die Aufklärung der Bevölkerung über Desinformation. Auch kann der Erlass von Gesetzen helfen, um die Verbreitung von Deepfakes zu kriminalisieren und Plattformen zu verpflichten, strenger gegen falsche Inhalte vorzugehen. Diese Maßnahmen können helfen, die Verbreitung von Desinformation zu verringern und die Integrität öffentlicher Diskurse zu schützen.

Aus Verbrauchersicht ist es nicht immer einfach, KI-Inhalte direkt als solche zu erkennen. Während noch vor Monaten Stimmen hallend, Bilder rauschend und Videos ruckelnd waren, sind diese Nebenerscheinungen in heutigen Fälschungen leicht umgehbar. Trotzdem gibt es neben der Überprüfung der Quelle zwei Anhaltspunkte, die zur Identifikation von KI beitragen können. Die einfachste Möglichkeit ist es, auf Merkmale zu achten, welche KIs typischerweise Schwierigkeiten bereiten. Eine hohe Fehleranfälligkeit tritt nämlich in folgenden Bereichen auf: Schatten, Reflexionen, leichte Abweichung der Hautfarbe im Hals- und Gesichtsbereich, unnatürliche Mundbewegungen verblasste beziehungsweise scharfe Ränder oder nahezu märchenhaft wirkende Aufnahmen ohne untypische Ereignisse im Hintergrund. Die zweite Möglichkeit ist technisch anspruchsvoller, aber dafür eindeutig. Die meisten großen und seriösen KI-Modelle hinterlassen ein Wasserzeichen, was durch technische Algorithmen zweifelsfrei nachweisbar ist, jedoch gibt es die Nachteile, dass dies aktuell noch einiges an technischen Wissen voraussetzt und darüber hinaus keine Fälschungen erkennen kann, die auf solche Identifikationsmöglichkeit bei der Erstellung verzichten. Somit ist die erste Möglichkeit die alltagstauglichste, welche für eine erste Einschätzung herbeigezogen werden kann.

Cyber attacks
Im Zeitalter von künstlicher Intelligenz und Big Data sind viele unserer Infrastrukturen schon verflochten mit Software und verbunden mit einer riesigen Menge von Daten. Aus diesem Grund zielen Cyberattacken auf kritische Infrastrukturen, wie die Energieversorgung, das Transportwesen, das Finanzwesen und den Regierungseinrichtungen ab und stellen eine ernsthafte Bedrohung dar.

Solche Angriffe können schwerwiegende Auswirkungen auf die nationale Sicherheit von Ländern haben und sind darauf hinaus, geheime oder sensible Informationen von Regierungen, Unternehmen oder anderen Organisationen zu stehlen, sei es, um sich einen strategischen Vorteil zu verschaffen oder um Lösegeld zu erpressen.

Ein weiteres großes Risiko stellt Cyber Propaganda dar, mit der Nutzung von Social-Media-Plattformen, gefälschten Nachrichten und anderen digitalen Mitteln, um die Öffentlichkeit zu manipulieren, beispielsweise im Kontext der Wahlmanipulation.

Damit stellt sich die Frage, wie man sich am besten schützt. Es muss davor betont werden, dass weder Staaten noch Unternehmen sich vollständig vor Cyberangriffen schützen können und stets mit der Möglichkeit eines Angriffs rechnen müssen. Die einzig praktikable Lösung ist eine umfassende und kontinuierliche Überprüfung der Systeme durch spezialisierte Cyber-Security Unternehmen.

Einfluss von Technologieunternehmen
Aufgrund der Tatsache, dass die bedeutendsten Technologieunternehmen der Welt von einzelnen Privatpersonen geführt werden, birgt dies für Unternehmen und Regierungen, die sich deren IT-Infrastruktur angenommen haben, eine Abhängigkeit geknüpft an die persönlichen Auffassungen des Eigentümers bzw. des Geschäftsführers.

Diese Abhängigkeit darf nicht nur monetär verstanden werden, sondern muss auch inhaltlich berücksichtigt werden. Abhängigkeit heißt nämlich nicht nur, an etwas gebunden zu sein, sondern hat auch die Nebenerscheinung, einen Teil der eigenen Macht zu verlieren, was bei kritischer Infrastruktur fatale Folgen haben kann. Mögliche Szenarien wären unautorisierte Zugriffe auf vertrauliche Daten oder absichtliche Störungen der IT-Systeme durch deren Bereitsteller, um die Arbeit zu behindern. Auslöser dafür können sowohl politischen als auch kommerziellen Ursprungs sein.

Um solche Situationen zu vermeiden, ist es wichtig, diesen Teilverlust der Verfügungsmacht bei der Wahl des Anbieters zu berücksichtigen. Die optimale Lösung besteht darin, die digitale Systemumgebung für die kritische Infrastruktur vom eigenen Staat in Form eines zentralen und selbst entwickelten Systems zu beziehen. Selbstverständlich muss man dabei auch auf hohe Sicherheitsanforderungen achten, welche einen entsprechenden Schutzfaktor erhöhen. Sofern man diese zwei Punkte berücksichtigt, kann man die Abhängigkeit von Privatpersonen und das damit einhergehende Missbrauchspotenzial deutlich reduzieren.

Konklusion
Die Cyber Diplomacy wird auch in der Zukunft weiter an Relevanz gewinnen, da die damit verbundenen Einsatzmöglichkeiten viele Erleichterungen schaffen. Doch wo Chancen sind, da trifft man auch auf Risiken. Risiken, die man auf keinen Fall missachten sollte, sondern zum Anlass nehmen, international an Normen zu arbeiten, um gemeinsame Regelungen festzulegen. Ebenso wichtig ist es, stets möglichst viel Einfluss über die eigene Infrastruktur für sich zu behalten und die digitale Sicherheit regelmäßig zu überprüfen.