DIE ERKENNUNG UND BEWÄLTIGUNG NEUER HYBRID- UND CYBER-SICHERHEITSHERAUSFORDERUNGEN – DAS ERSTELLEN DER BELASTBAREN KRITISCHEN INFRASTRUKTUR

Stärkung der Demokratie, Schutz der Freiheit und der Gesellschaft

Es gibt drei Ansätze für den Umgang mit hybriden Bedrohungen:

I. Wissenschafts-Technologischer, basierend auf einer Stellungnahme zur Wirksamkeit der Technologie und der Voraussetzung, dass bessere Technologien Bedrohungen wirksam begegnen können. Technologien können, und sind, in meisten Fällen Entwicklungstechnologien. Ihr Hauptproblem ist jedoch, dass auch die besten Technologielösungen von den Menschen die sie erstellen, verwenden und interpretieren, abhängen. Ein menschlicher Faktor ist sehr oft zu selbstbewusst in die eigenen Fähigkeiten, ist ungenügend erfahren und geschult, um die Unvollkommenheit des Systems zu erkennen oder einfach nicht in der Lage ist, genaue und zeitnahe Entscheidungen zu treffen.

II. Theoretischer Ansatz entwickelte sich zwischen dem strategischen und dem taktischen Konzept, indem betont wird, dass eine bessere Planung eine bessere und effektivere Verteidigung bietet.

Die drei Schlüsselelemente des theoretischen Konzepts sind: Prävention, Ernennung und Reaktion.

- **PRÄVENTION**

Die klassischen Formen präventiver Maßnahmen basieren sich auf den Gelegenheiten, Fähigkeiten und der Bereitschaft, konventionelle militärische

This workshop is supported by: The NATO Science for Peace and Security Programme

Verteidigungsgeräte nach Bedarf einzusetzen. Heutzutage sind jedoch die klassische Verteidigungsgeräte, mit denen die Staaten verfügen, irrelevant für moderne Konflikte oder ihre Anwendung stellt keine Lösung für die meisten Missverständnisse dar (war das Vereinigte Königreich oder Spanien bereit, in bewaffnete Konflikte um Territorialgewässer um Gibraltar oder Gibraltar selbst einzutreten?). Heute ist es wichtig, die Frage zu stellen, wie ein wirksamer präventiver Schutz in der digitalen Welt organisiert werden kann. Können wir Einzelpersonen, Gruppen und Staaten davon abhalten, unsere individuellen oder gemeinsamen Interessen und Ziele in der digitalen Welt anzugreifen? Ist die Prävention an sich ausreichend?

- **ERNENNUNG**

In den vergangenen Jahrzehnten war es leicht, die Quelle der Aggression sowie ihre Initiatoren zu bestimmen. Der Angegriffene wusste, weil er sah und fühlte, wer ihn angrifft, wie, mit was und wo. Heute ist das Problem des Cyber-Angriffs äußerst gut verdeckt (insbesondere im Hinblick auf institutionelle Angreifer) und versteckt. Es ist sehr oft der Fall, dass jemand, der von Hybridangriffen (oder Cyberangriffen) angegriffen wird, sich dessen gar nicht bewusst ist. Selbst wenn der Angegriffene sich der Angriffe durch Hybridangriffe bewusst ist, kann häufig nicht ermittelt werden, wer wirklich hinter dem Angriff steht, da wer der Angreifer ist, wer der Planer und / oder der Veranstalter ist. Es ist daher notwendig, die Aktivitäten die sich auf das Erkennen des Angreifers und seine zuverlässige und eindeutige Ernennung als Bedrohungsquelle zu konzentrieren, den Angegriffenen zur Verfügung zu stellen. Zu diesem Zweck ist es notwendig, intensiv zu arbeiten und die Fähigkeiten und das Wissen des Staates, des öffentlichen, privaten und akademischen Sektors zu integrieren, um Wege, Modelle, Methoden und Ressourcen zu finden, um Hybridangriffe zuverlässig benennen zu können. Die

NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

Existenz eines solchen Systems ist eine der besten Möglichkeiten, einen Angriff zu verhindern.

- **REAKTION**

In der Zeit, als das Ernennen des Angreifers eindeutig war, konnte die Antwort mit den geeigneten Mitteln auf den identifizierten Angreifer angepasst werden. Wenn man sich heute die große Verschwörung von Hybridangriffen und Angreifern ansieht, ist es in der Tat sehr anspruchsvoll und manchmal mit den üblichen Methoden und Mitteln fast unmöglich zu bestimmen, wer hinter dem Angriff steht und an wen, auf welche Weise, wo und wie zu reagieren ist. Doch, in gewisser Weise muss ein Angriff beantwortet werden. Gespräche über die Notwendigkeit der Existenz und Entwicklung besonders defensiver und vor allem angreifender Spezialisten, insbesondere in der Cyberwelt, werden äußerst unnötig, unproduktiv und schädigen sogar der Organisation einer wirksamen Verteidigung. Die Entwicklung integrierter Systeme und Modelle der aktiven Verteidigung und geeigneter technologischer Lösungen weist auf eine neue Realität hin. Eine neue Realität erfordert die Diskussion neuer ethnischer Fragen sowie die Notwendigkeit, Hybridregeln zu definieren, insbesondere des Cyberkriegs. Wie hoch ist die Sicherheit der Ernennung eines echten Angreifers, der eine angemessene Reaktion in Form der Aktivierung seiner eigenen Wirkung einleiten kann; soll man auf ein Cyberangriff auf eine Institution oder ein Unternehmen (und auch privat) in seinem eigenen Gebiet mit den aktiven Verteidigungsgeräten, die dem Staat verfügbar sind, antworten; was muss man tun, wenn eine Person angegriffen wird? Wie kann man den eigenen Informations- und Kommunikationsraum und die eigene informations- und digitale

NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

Souveränität schützen, um die Werte der demokratischen Gesellschaft und die Rechte und Freiheit von Individuen und Gemeinschaft zu erhalten?

Wie hoch ist der Grad der Reaktion, auch wenn der Angreifer zuverlässig ernannt wird und zu welchen Zielen? Soll man auf einen Angriff mit einer digitalen Waffe, eine Antwort initiieren mit der Benutzung des digitalen Flugzeugträgers und der gesamten digitalen Flotte?

Klar ist, dass es solche Regeln noch nicht gibt, denn die Herausforderungen, denen wir gegenüberstehen, sind technologisch revolutionärer als die evolutionäre Natur (ein Beispiel für komplexe Computer-Schadprogramme wie STUXNET und FLAME).

III. Praktischer Ansatz betont die Notwendigkeit, ein zuverlässiges System für ein wirksames Krisenmanagement, die Entwicklung anpassungsfähiger Strukturen und Krisenmanagementverfahren, aufzubauen. Das Vorhandensein wirksamer Krisenmanagementstrukturen, die regelmäßige, qualitative und reale Schulungs- und Trainingsprozesse durchlaufen, bedeutet, dass selbst die am wenigsten erwartete (oder unerwartete) Krise eine qualitative und zuverlässige Reaktion hervorbringen kann. Eines der Hauptbedürfnisse dieses Systems ist die Notwendigkeit, ein effektives Krisenkommunikationsmodell zu entwickeln.

Probleme, Sicherheitsbereiche, gelernte Lektionen, Empfehlungen

1. Hybride Bedrohungen sind eine reale und gegenwärtige Bedrohung. Hybride Bedrohungen und Krisen erfordern auch hybride Reaktionen, die nicht nur auf technischen und technologischen Fähigkeiten beruhen, sondern auch Krisenmanagementsysteme einbeziehen.

2. Das Krisenmanagement muss unter möglichst realistischen Bedingungen geplant, geschult und regelmäßig geübt werden. Nur auf Technologie zu setzen, garantiert nicht Erfolg, sondern Misserfolg. Ein menschlicher Faktor ist ebenso wichtig wie eine technologische Lösung.

NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

3. Internationale Zusammenarbeit ist kein Luxus, sondern eine Notwendigkeit. Dies ist ein untrennbarer Bestandteil der Reaktion, da es sich bei hybriden Bedrohungen nicht nur um lokale und regionale, sondern auch um globale Bedrohungen handelt. Daher muss die Antwort dieselbe sein.

4. Selbsthilfelösungen erschweren oder verunmöglichen die internationale Zusammenarbeit, gleich wie die Fragmentierung und Eindeutigkeit von Institutionen innerhalb einzelner Staaten und Gemeinschaften. Wir weisen auf einen erhöhten Bedarf an Standardisierung und das allgemeine akzeptierten von Sicherheitsverfahren, Protokollen und Zertifikaten hin.

5. Die technologische Entwicklung muss sich auf vier Kernkompetenzen konzentrieren: Interoperabilität, Schulung und Zertifizierung.

6. Staatliche Institutionen, Ministerien und Agenturen konkurrieren um Haushaltsmittel mit dem Ziel, ihre eigenen, im Bereich hybrider Aktionen wirksamen Mittel zu entwickeln. In der Wirklichkeit befinden sich rund 80% des Sektors für kritische Infrastruktur in den Industrieländern in den Händen privater Eigentümer und werden von privaten Sicherheitsunternehmen geschützt. Daher sollte der Privatsektor als zumindest gleichberechtigter Partner bei der Entwicklung und Umsetzung von Strategien und Taktiken für den Umgang mit hybriden Bedrohungen verstanden und akzeptiert werden. In diesem Sinne ist es in diesem Tätigkeitsbereich auch notwendig, die akademische Gemeinschaft mit ihren Kenntnissen und Fähigkeiten einzubeziehen.

7. Das Ausbildungssystem sollte nicht innerhalb nationaler Rahmenbedingungen eingeschränkt werden. Der Aufbau grenzüberschreitender Schulungen sollte auf ähnliche Weise entwickelt werden, wie bereits ein Katastrophenmanagementsystem eingerichtet wurde.

8. Hybride Bedrohungen in Form von Operationen, die demokratische Gesellschaften betreffen, insbesondere im Bereich böswilliger Einflüsse auf Wahlen, erfordern die

Entwicklung von sozialem Widerstand. Sie muss auf dem persönlichen, aber auch gemeinsamen Ansatz des akademischen, staatlichen, öffentlichen und privaten Sektors beruhen.

9. Desinformationsaktivitäten erfordern eine gewisse Vorbereitungszeit, um wirksam zu sein. Wie in den Absätzen 3 und 6 hervorgehoben wurde, sollte der positive Effekt ihrer Zusammenarbeit in der Entwicklung einer wirksamen und zuverlässigen künstlichen Intelligenz für die Bedürfnisse von Aktivitäten im Bereich der sozialen Netzwerke sichtbar werden. Ziel ist es, hybride Bedrohungen und Angriffe zu identifizieren und Angreifer in einem frühen Stadium der Planung und Aktion zu ernennen. Diese Instrumente, die von der nationalen und der Vereinigung (internationale Organisationen, deren Mitglied der Staat ist) entwickelt und unterstützt werden, sollten als System zur Frühwarnung vor Bedrohungen dienen.

10. Das gemeinsame Handeln des Staates, des öffentlichen, des privaten und des akademischen Sektors auf dem Gebiet der Entwicklung im Bereich der Information- und der digitalen Kompetenz und des kritischen Denkens, ist eine notwendige Voraussetzung für das Erreichen des Status der Information- und der digitalen Souveränität auf nationaler und internationaler Ebene. Ziel ist die Wahrung der Demokratie sowie die Wahrung und Weiterentwicklung der Rechte und Freiheiten des Einzelnen und der Gesellschaft.

11. Es ist notwendig, ein System von international anerkannten und akzeptierten Regeln oder Konventionen des digitalen Konfliktes zu entwickeln, die möglich sein wird, sie implementieren oder die Umsetzung und Einhaltung zu erzwingen. Hybride Konflikte sollten als Mittel zur Massenvernichtung behandelt werden.

NATO OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

Hybrid Warfare Research Institute

Udruga Sv. Jurja St. George Association

Zagreb Security Forum 2020

Zagreb, 13./14. März 2020

This workshop is supported by: The NATO Science for Peace and Security Programme

This workshop is supported by: The NATO Science for Peace and Security Programme