TUM THINK TANK

Digital Sovereignty Talks

Food4Thought

Winter 2024

Munich School of Politics and Public Policy (HfP) · TUM Think Tank

v1.5

Digital Multilateralism and the Fight against Cyber Crime - Learnings from the German Federal Criminal Police Office [Article in German]

By Sofie Schönborn and Philipp Mueller

In our last session, we learned that cybercrime operates across borders, demanding a collaborative and transnational response. The German Federal Criminal Police Office (BKA) has demonstrated how strategic initiatives, advanced technologies, and effective leadership can enhance efforts to combat these threats. By implementing a "Cyberfighting-as-a-Service" model, fostering strong international partnerships, and prioritizing talent development, the BKA not only improves Germany's digital security but also contributes significantly to global cybersecurity initiatives. [Article in German]

In der heutigen vernetzten Welt überschreitet Cyberkriminalität nationale Grenzen und erfordert einen ebenso transnationalen Ansatz, um sie wirksam zu bekämpfen. Das deutsche Bundeskriminalamt (BKA) hat sich als führende Kraft auf diesem Gebiet herausgestellt und gezeigt, wie gemeinsame Anstrengungen und starke Führung die Cybersicherheit und damit die nationale Souveränität erheblich verbessern können. Dieser Artikel befasst sich damit, wie die strategischen Initiativen des BKA, der Einsatz fortschrittlicher Technologien und die Stärkung der Führung es zu einem wichtigen Akteur im Kampf gegen Cyberkriminalität gemacht haben.

Die transnationale Natur der Cyberkriminalität

Cyberkriminalität kennt keine Grenzen. Kriminelle agieren weltweit und nutzen hochentwickelte Netzwerke und Technologien, um Verbrechen zu begehen, die Einzelpersonen, Unternehmen und Regierungen weltweit betreffen. Die Professionalisierung der Cyberkriminalität hat zu „Cyberkriminalität als Dienstleistung" geführt, bei der illegale Dienste auf Schwarzmarktplattformen gehandelt werden. Dieser Wandel erfordert einen ebenso professionellen und kollaborativen Ansatz zur Bekämpfung der Cyberkriminalität, wie ihn das „Cyberfighting-as-a-Service"-Modell des BKA veranschaulicht.

Die Rolle des BKA bei der Bekämpfung der Cyberkriminalität

Das BKA fungiert als zentrale Anlaufstelle für die 16 deutschen Länderpolizeien sowie den europäische und internationale Polizeibehörden und sammelt Daten und Wissen, um die bundesweite Kriminalitätsbekämpfung zu unterstützen. Durch die Einführung eines „Cyberfighting-as-a-Service"-Ansatzes erleichtert das BKA eine koordinierte Reaktion auf Cyberbedrohungen und ermöglicht es so, dass selbst die kleinsten Polizeidienststellen Zugang zu Spitzentechnologie und Fachwissen haben. Dieses Modell erhöht nicht nur die innere Sicherheit Deutschlands, sondern stärkt auch seine Position in globalen Cybersicherheitsnetzwerken.

Viele bemerkenswerte Erfolge des BKA wie z.B. die Operation Endgame, sind koordinierte Aktionen mit internationalen Partnern. Hierdurch konnten cyberkriminelle Netzwerke aufgedeckt werden, die an der Verbreitung von Malware beteiligt waren. Verhaftungen und Beschlagnahmung von Drogen, Waffen Kryptowährungen oder Bargeld, die Abschaltung von Infrastrukturen sind regelmäßig die Folge. Diese Operationen unterstreichen die Macht multinationaler Zusammenarbeit, bei der der

Austausch von Informationen, Ressourcen und Fachwissen zu bedeutenden Siegen gegen raffinierte Cyberkriminelle führen kann.

Die Beteiligung des BKA an solchen Operationen unterstreicht sein Engagement für den Schutz digitaler Infrastrukturen und die Eindämmung von Cyberbedrohungen auf globaler Ebene.
Die technologische Kompetenz des BKA ist ein entscheidender Bestandteil seines Erfolgs. Die Agentur beschäftigt Experten, die sich mit den neuesten Cloud-Diensten und Open-Source-Tools auskennen, sodass sie die erforderliche Software schnell erstellen und bereitstellen können. Diese Fähigkeit zur Selbstbedienung aus einer Vielzahl technologischer Ressourcen stellt sicher, dass das BKA an der Spitze der Cybersicherheitsinnovationen bleibt.

Führung: Fünf Schlüssel zum Erfolg

Der Eckpfeiler der Effektivität des BKA ist jedoch seine Führung, die der Befähigung kleiner und agiler Teams Priorität einräumt. Führungskräfte auf allen Ebenen, vom Präsidenten über Abteilungsleitungen bis zu den operativen Teams, arbeiten daran, behördliche bürokratische Hürden abzubauen und die erforderlichen Ressourcen bereitzustellen, damit ihre Teams hervorragende Leistungen erbringen können, während sie gleichzeitig Compliance und Vertrauen aufrechterhalten. Dieser Ansatz fördert ein Umfeld, in dem Innovationen gedeihen und Teams schnell auf neue Bedrohungen reagieren können.

1. Unterstützung von oben: Die Führung des BKA ist geprägt von der Verpflichtung, Freiräume für Ihre Teams zu verteidigen und sie dabei zu unterstützen, schnelle und eigene Entscheidungen zu treffen. Eine solche Führung stärkt nicht nur die Moral, sondern stellt auch sicher, dass die Teams die Freiheit und Unterstützung haben, die sie brauchen, um sich in komplexen und sich ständig verändernden Cyberlandschaften zurechtzufinden.

2. Partnerschaften zur Stärkung der digitalen Souveränität: Die digitale Souveränität Deutschlands wird durch seine multinationalen Partnerschaften erheblich gestärkt. Durch die Zusammenarbeit mit globalen Cybercrime-Agenturen und die Teilnahme an gemeinsamen Operationen nutzt das BKA kollektives Fachwissen und Ressourcen, um Cyberbedrohungen zu bekämpfen. Diese internationale Zusammenarbeit ist von entscheidender Bedeutung, um der dynamischen Natur der Cyberkriminalität zu

begegnen und Deutschlands Position in der globalen Cybersicherheitslandschaft zu stärken.

3. Das digitale Ökosystem mitgestalten: Die Bekämpfung der Cyberkriminalität ist nicht mehr nur eine Aufgabe der nationalen Polizei, sondern erstreckt sich über nationale Grenzen hinaus bis in den privaten Sektor. Die Bemühungen des BKA reichen über Grenzen hinaus und beeinflussen das breitere digitale Ökosystem. Durch Partnerschaften mit internationalen Agenturen wie Europol und Interpol sowie durch die Zusammenarbeit mit dem privaten Sektor spielt Deutschland eine entscheidende Rolle bei der Gestaltung von Standards und Praktiken der Cybersicherheit. Die Operation EncroChat, bei der eine sichere Kommunikationsplattform der organisierten Kriminalität infiltriert und entschlüsselt wurde, zeigt die Zusammenarbeit zwischen deutschen, französischen, niederländischen und Europol-Partnern beim Abfangen von Millionen krimineller Nachrichten, was zu zahlreichen Festnahmen und der Zerschlagung illegaler Netzwerke in ganz Europa führte. Dieser kollaborative Ansatz trägt dazu bei, eine sicherere und widerstandsfähigere digitale Umgebung für alle Beteiligten zu schaffen.

4. Entscheidungsträger stärken: Durch die Modernisierung der digitalen Infrastruktur und die Verbesserung der Fähigkeiten des BKA können Entscheidungsträger wirksam auf Cyberbedrohungen reagieren. Die CyberToolbox, eine intern entwickelte Plattform mit Open-Source-Komponenten, ist ein Beispiel für das Engagement des BKA für Selbständigkeit und Datensicherheit. Indem das BKA die Kontrolle über seine digitalen Tools behält, gewährleistet es robuste und anpassungsfähige Cybersicherheitsmaßnahmen.

5. Talente entwickeln und halten: Qualifizierte Mitarbeiter sind für die Wahrung der digitalen Souveränität von entscheidender Bedeutung. Der Fokus des BKA auf kontinuierliche Kompetenzentwicklung und innovative Einstellungspraktiken wie gezielte Rekrutierungstage und Jobrotationen unterstreicht die Bedeutung der Gewinnung und Bindung von Talenten in Schlüsselbereichen wie KI, Cybersicherheit und Cloud-Management. Die Gewährleistung einer robusten Talentpipeline ist unerlässlich, um in der sich schnell entwickelnden digitalen Landschaft die Nase vorn zu behalten.

Fazit

Der Erfolg des BKA im Kampf gegen Cyberkriminalität basiert auf der Kraft der Zusammenarbeit, modernster Technologie und der Stärkung der Führung. Durch die Einführung eines „Cyberfighting-as-a-Service“-Modells verbessert das BKA nicht nur die innere Sicherheit Deutschlands, sondern trägt auch zu den weltweiten Bemühungen um Cybersicherheit bei. Die Erkenntnisse aus dem Ansatz des BKA – Förderung multinationaler Partnerschaften, Modernisierung der digitalen Infrastruktur und Entwicklung qualifizierter Talente – unterstreichen die Bedeutung dieser Elemente für die Stärkung der digitalen Souveränität und die wirksame Bekämpfung der Cyberkriminalität.