IGF 2025 - Day 2 - Wednesday June 25, 2025, 12:00 - 13:00 CEST - Workshop Room 6

NRIs Collaborative Session: ローカルな実践を通じたグローバルなサイバー脅威への対処

サイバーセキュリティの課題は地球規模で拡大し、2025 年には世界のサイバー犯罪による年間被害額は 10.5 兆ドルに達すると予測されています。このセッションでは、各国および地域の**マルチステークホルダー**による協力が、より強固で回復力のあるサイバーセキュリティフレームワークを構築し、同時にイノベーション、セキュリティ、人権保護のバランスをどのように取るかを探求しました。

主な焦点と議論のポイント

- **規制とプライバシーの間の緊張**: サイバーセキュリティ法と既存のプライバシーおよびデータ保護対策との間の緊張関係に重点が置かれました。
- **規制の影響**: DNS オペレーターなどのサービスプロバイダーに対するより厳格な規制が、かえって効果的なセキュリティメカニズムを損なう可能性について議論されました。
- **コストと便益**: 追加の規制がデジタルセキュリティ全体を強化するかどうか、またサービスプロバイダーやエンドユーザーにどのようなコストを課すかについて検討されました。
- **地域の実践**: 各国および地域の**インターネット・ガバナンス・フォーラム（NRI）**の経験が共有され、ガバナンス、説明責任、インシデント対応への多様なアプローチが強調されました。
- **サイバー犯罪対策**: 組織的サイバー犯罪の脅威、犯罪ネットワークの進化、および法執行機関に求められる新しい能力についても議論されました。
- **人権の尊重**: 包括的なインターネットガバナンスがグローバルなサイバーセキュリティを強化し、法律と技術が人権を擁護することを確実にし、効果的な法制化、法執行能力、および国民の意識向上を通じて新たなサイバー脅威に対処する方法が探求されました。

目的

このセッションは、具体的な実践例を通じて、さまざまな状況でサイバーセキュリティのレジリエンスを強化するための具体的で協力的な道筋を特定することを目的としています。対話と意見交換を通じて、サイバー脅威に対抗し防止する方法に焦点を当てました。

共同主催者

- セルビア IGF の Dijana Milutinovic 氏
- ガーナユース IGF の Lily Botsyoe 氏
- シンガポール IGF の Henry Wang 氏と Una Wang 氏
- ガーナ IGF の Godsway Kubi 氏
- IGF ポルトガルの Tiago Martins 氏
- 日本 IGF の Shin Yamasaki 氏
- アルゼンチン IGF の Agustina Ordonez 氏
- オランダ IGF の Dorijn Boogaard 氏
- コロンビア IGF の Ximena Estefania Riano Agudelo 氏と Aristides Contreras Fernandez 氏
- LACIGF の Lilian Chamorro 氏

一般参加者が発言する前に登壇する専門家パネル

- Mr. Carlos Vera, Director Ejecutivo, ISOC Ecuador, IGF Ecuador
- Mr. Dejan Đukić, CEO, RNIDS, Serbia IGF
- Ms. Lia Hernandez, Founder of Ipandetec, Panama IGF
- Mr. Dennis Broeders, Professor of Global Security and Technology, Senior Fellow at The Hague Program on International Cyber Security, Institute of Security and Global Affairs, Leiden University; Project Coordinator, EU Cyber Direct, The Netherlands IGF
- Ms. Latty Thlaka, Chairperson of the ZAIGF Multistakeholder Committee, South Africa IGF

セッションの流れ

- Welcome by the moderator and introduction (5 min)
- Setting the stage by designated and endorsed speakers (20 min)
- Open floor discussion (20 min)
- Conclusion and closing (5 min)

現地モデレーター: Ms. Jennifer Chung, APrIGF

オンラインモデレーター: Godsway Kubi, Lead facilitator, Internet Society Online Safety SIG, Ghana IGF

報告者: Ms. Ines Hfaieda from Tunisa and Phyo Thiri Lwin, Myanmar Youth IGF

セッション概要

このセッションは、「地域の実践を通じたグローバルなサイバー脅威への対処」と題され、増大するサイバーセキュリティの課題に対して、**マルチステークホルダー**なアプローチと地域レベルでの協力を通じてどのように対応していくかに焦点を当てました。特に、サイバーセキュリティ法とプライバシー・データ保護の間の緊張関係、そしてAIやIoTといった新興技術がもたらす影響が議論されました。

主要な論点と提言

1. **AIとIoTにおけるサイバーセキュリティの懸念:**
    - **データプライバシーと悪用**: AI・IoT デバイスは大量の情報を収集しますが、デジタルリテラシーが低い地域では、ユーザーの理解や同意なしにデータが収集されるリスクがあります。これにより、監視、プロファイリング、意図的な危害の可能性が生じます。
    - **脆弱なインフラ**: 地方自治体や小規模組織は、サイバー攻撃、特にランサムウェアの標的となりやすい脆弱なデジタルシステムを抱えていることが多いです。
    - **信頼と不平等**: AIシステムの障害は信頼の喪失につながり、脆弱なコミュニティ（マイノリティや低所得者層）が最も影響を受けやすいです。
    - **提言**:
        - **セキュリティ・バイ・デザイン**: AIおよびIoTシステムは最初から安全に設計されるべきです。
        - **地域社会のエンパワーメント**: 大企業だけでなく、市民、地域住民、地域のリーダーなど、システムを管理・維持する人々へのトレーニングと能力開発に投資すべきです。
        - **参加型ガバナンス**: 市民がAIとIoTの利用方法を形成するプロセスに、**マルチステークホルダー**が参加することが不可欠です。
        - **地域行動のためのグローバルフレームワーク**: 一律の解決策ではなく、地域の現実を考慮した政策が必要です。最終利用者だけでなく、政府や企業にも倫理的な行動が求められます。
2. **厳格な規制とセキュリティ、コスト**:
    - **規制の遅さ**: サイバー脅威の高度化に対し、規制の進化は技術の進化に追いついていません。

- **プライバシーとセキュリティのバランス**: 厳格な規制（例: GDPR や NIS2 指令）は、セキュリティを向上させる一方で、個人データ収集の増加やプライバシーとの間の難しいバランスを要求します。
- **コスト**: 厳格な規制は、サービスプロバイダーのシステム改善や、エンドユーザーの新しいシステムへの適応にコストを伴います。
- **協力の重要性**: DNS オペレーターの事例（例: セルビアの RNIDS）から、サイバー犯罪対策には、登録事業者、警察、検察当局など、関係者間の協力と関連データ・知識の共有が不可欠であることが示されました。

3. **サイバー犯罪対策における政策アプローチと教育**:
   - **国家政策としてのサイバーセキュリティ**: サイバーセキュリティやサイバー犯罪への取り組みは、政府交代によって優先順位が変わらないよう、国家政策として位置づけられるべきです。
   - **法整備の遅れ**: 国際的なサイバー犯罪条約（例: 新しい国連サイバー犯罪国際条約）が批准されても、国内法への反映が遅れることがあります。
   - **教育の重要性**: 子供から高齢者まで、インターネットがどのように機能し、誤った利用がどのような結果を招くかを説明することが重要です。単に「してはいけない」と伝えるのではなく、リスクを識別できるように教育すべきです。
4. **サイバーセキュリティ情報の共有とレジリエンス**:
   - **情報共有の障壁**: デジタル脆弱性や脅威に関する情報共有は、その価値が認識されつつも、実践は困難です。情報を持つ組織（諜報機関、企業など）は、機密保持、責任問題、ビジネスモデルといった理由から共有に消極的です。
   - **信頼コミュニティの構築**: **CSIRTs**（コンピューターセキュリティインシデント対応チーム）のように、国際的な情報共有の長い伝統を持つ組織や、金融セクターの **ISAOs**（情報共有・分析組織）のような信頼コミュニティを構築することが効果的です。政府は、このような情報共有の促進において重要な役割を果たすことができます。
   - **「ヘルス＆セーフティ」アプローチ**: 責任追及ではなく、「ヘルス＆セーフティ」の観点から情報共有を促し、患者の安全を優先する医療現場のようなアプローチをサイバーセキュリティにも適用することが提案されました。
5. **地域の実践とグローバルな協力**:
   - **マルチステークホルダーアプローチ**: サイバーセキュリティは、技術的な課題だけでなく、人権、開発、ガバナンスの問題でもあります。そのため、国家、地域、グローバルレベルでの**マルチステークホルダー**協力が不可欠です。

- **地域主導の取り組み**: バングラデシュ IGF やナイジェリア IGF の例に見られるように、地域社会に基づいた能力開発と**マルチステークホルダー**の関与は、トップダウンアプローチよりも効果的にサイバー脅威に対処できます。
- **地元の才能の活用**: 大学で育成される地元の人材やスキルが、サイバー脅威対策に十分に活用されていない現状が指摘され、これらの資源の活用が提言されました。
- **法の執行機関の強化**: グローバルサウスにおける法の執行機関の能力強化が、サイバー脅威への効果的な対応に不可欠であるとされました。
- **サイバーセキュリティと人権**: 南アフリカ IGF は、サイバーセキュリティ法とプライバシー・データ保護の人権としての憲法上の義務との間に生じる緊張関係を強調しました。サイバーセキュリティ戦略は、プライバシー保護と人権ベースのガバナンスと連携すべきです。監視における透明性と説明責任を確保し、若者や市民社会を含むインクルーシブなガバナンスを推進することが重要です。

まとめ

このセッション全体を通じて、サイバー脅威が地球規模で増大し、その複雑性が高まっていることが強調されました。しかし、その対応は地域の現実に基づき、地域主導で行われる必要があります。資金調達、多様なステークホルダーの巻き込み、法的枠組みの整備、そして一般市民への教育といった課題に対して、NRI がそのマルチステークホルダーな性質を活かし、情報共有、協力、能力開発を通じて取り組んでいることが示されました。特に、企業が公共の利益のために情報を共有するインセンティブが不足していることや、規制の必要性が浮き彫りになりました。

最終的に、サイバーセキュリティは単にネットワークを守るだけでなく、人々の民主主義と尊厳を守ることであるという、根本的なメッセージが共有されました。NRI は、この複雑な課題に取り組む上で、地域レベルでの実践とグローバルな協力の架け橋となる重要な役割を担っています。