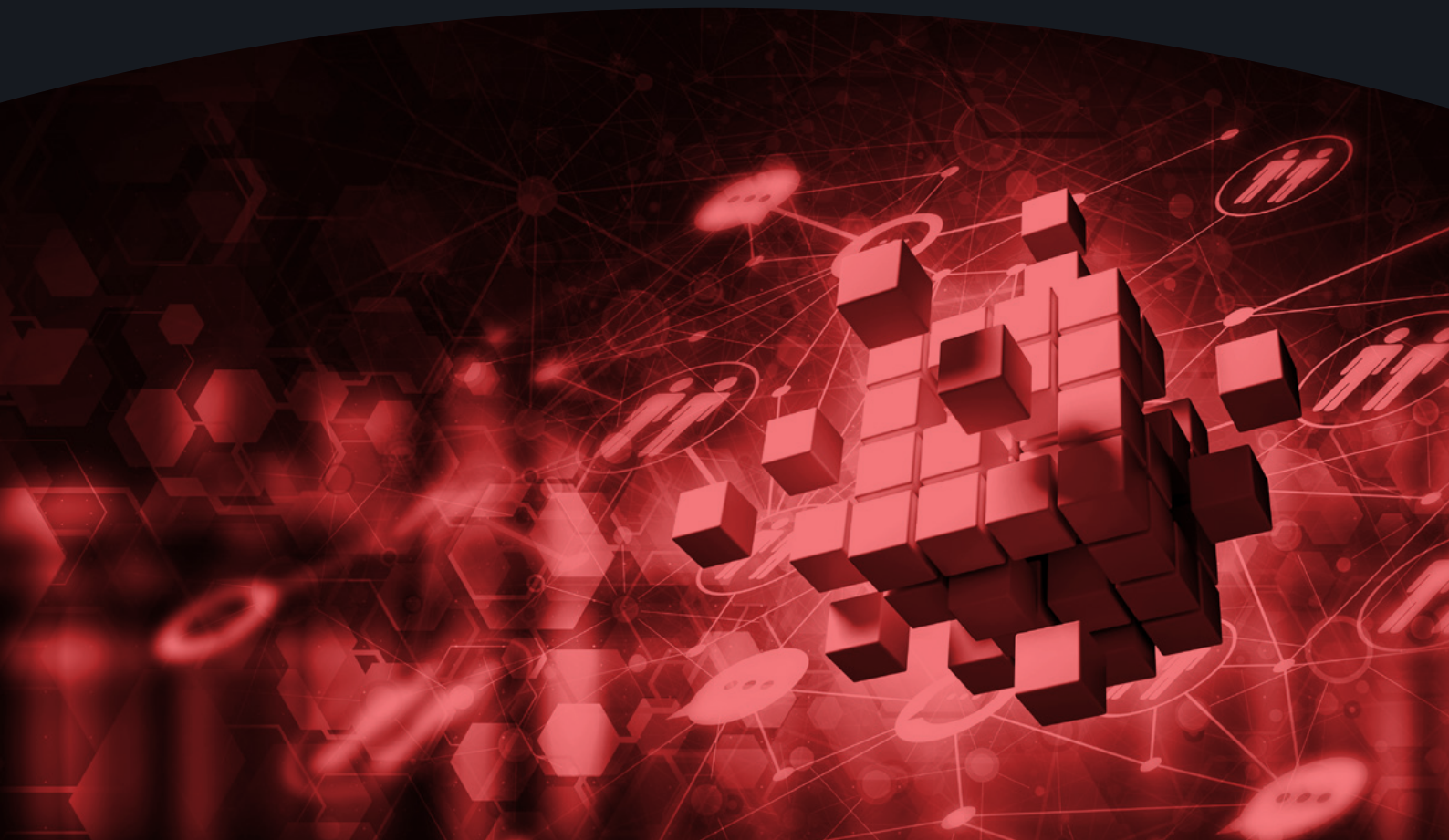
UNIDIR

O que é necessário para construir capacidades cibernéticas?

Parte II. Introdução a uma Abordagem Baseada em Ameaças

SAMUELE DOMINIONI · GIACOMO PERSI PAOLI



Obrigado

Pelo apoio dos principais contribuintes do UNIDIR que sustentam todas as atividades do Instituto. Este estudo faz parte do fluxo de trabalho de estabilidade cibernética do Programa de Segurança e Tecnologia UNIDIR, financiado pela Microsoft e pelos governos da República Tcheca, França, Alemanha, Itália, Holanda, Suíça e Reino Unido.

O UNIDIR deseja expressar sua gratidão ao Programa de Segurança Cibernética do Comitê Interamericano contra o Terrorismo (CICTE) da Organização dos Estados Americanos (OEA) por traduzir esta pesquisa e disponibilizá-la em português. Este relatório foi inicialmente publicado em julho de 2023 em inglês, que permanece a versão oficial. Em caso de divergência, o texto em inglês prevalecerá.

Sobre UNIDIR

O Instituto das Nações Unidas para Pesquisa de Desarmamento (UNIDIR) é um instituto autônomo das Nações Unidas financiado por contribuições voluntárias. O UNIDIR, um dos poucos institutos de políticas do mundo com foco no desarmamento, gera conhecimento e promove o diálogo e a ação sobre desarmamento e segurança. Com sede em Genebra, o UNIDIR auxilia a comunidade internacional no desenvolvimento de ideias práticas e inovadoras necessárias para encontrar soluções para problemas críticos de segurança.

Observação

Os Autores

Samuele Dominioni

Pesquisador, Programa de Segurança e Tecnologia

O Dr. Samuele Dominioni é pesquisador do Programa de Segurança e Tecnologia da UNIDIR. Antes de ingressar na UNIDIR, ocupou cargos de pesquisa em ambientes acadêmicos e de grupos de especialistas. É PhD em relações internacionais e história política pela Sciences Po, na França, e pela Escola de Estudos Avançados do IMT, na Itália.

Giacomo Persi Paoli

Diretor do Programa, Segurança e Tecnologia

O Dr. Giacomo Persi Paoli é o Diretor do Programa de Segurança e Tecnologia da UNIDIR. Seu conhecimento especializado abrange ciência e tecnologia com ênfase nas implicações de tecnologias emergentes para segurança e defesa. Antes de ingressar na UNIDIR, Giacomo foi Diretor Associado da RAND Europe, onde liderou o portfólio de ciência, tecnologia e inovação de defesa e segurança, bem como o Centro de Estudos de Prospecção da RAND. Ele é Ph.D. em Economia pela Universidade de Roma, Itália, e mestre em Ciência Política pela Universidade de Pisa, Itália.

Tabela de Conteúdo

Abreviações e Acrônimos

CBM	Medidas de construção de confiança
CERT/CSIRT	Equipe de Resposta a Emergências Informáticas/Equipe de Resposta a Incidentes de Segurança Informática
DDOS	Negação de serviço distribuída
FCC	Capacidades Cibernéticas Fundamentais
GEG	Grupo de Especialistas Governamentais
TIC	Tecnologia da informação e comunicação
LI	Lei internacional
OEWG	Grupo de trabalho aberto
UNIDIR	Instituto das Nações Unidas para Pesquisa de Desarmamento
ONUDA	Escritório das Nações Unidas para Assuntos de Desarmamento

Sumário Executivo

Embora os Estados continuem a discutir os quatro pilares principais do Marco para o Comportamento Responsável do Estado no Uso das TIC (doravante o Marco) - normas de comportamento responsável, direito internacional, medidas de fortalecimento da confiança e capacitação – há dois aspectos principais que ainda não foram explorados:

a. até que ponto a implementação do Marco pode ser usada para aumentar a segurança nacional, regional e internacional e resiliência contra ameaças específicas; e
b. como usar ameaças específicas para informar iniciativas de capacitação.

O cenário de ameaças no âmbito das TIC está em constante evolução, tornando-se mais complexo e sofisticado à medida que as medidas de cibersegurança continuam a melhorar. Embora deva ser observado que mais de noventa por cento dos ataques cibernéticos podem ser evitados por meio da aplicação consistente de “higiene” de segurança básica, o Marco pode fornecer uma importante camada adicional de resiliência. De fato, estabelecer as capacidades necessárias para implementar o Marco equiparia os Estados com ferramentas importantes que podem contribuir para a prevenção ou mitigação de ciberameaças específicas, bem como para fortalecer sua resiliência cibernética geral.

Este relatório é o segundo de um estudo em duas partes realizado pelo UNIDIR e visa fortalecer os vínculos entre o Marco e as capacidades dos Estados para prevenir ou mitigar efetivamente o

impacto de atividades maliciosas relacionadas às TIC. O relatório centra-se no conceito de Capacidades Cibernéticas Fundamentais (FCC, por suas siglas em inglês), introduzido na primeira parte do estudo, que é definido como a mistura de políticas e regulamentos, processos e estruturas, alianças e redes, pessoas e habilidades e tecnologia necessária para implementar o Marco.

Este relatório propõe uma abordagem que permitiria aos governos avaliar melhor sua preparação para aproveitar o Marco para prevenir ou responder a atividades e ameaças maliciosas específicas de TIC. A proposta de "abordagem baseada em ameaças" compreende três etapas.

- **Etapa 1. Avaliação de ameaças e riscos:** Nesta etapa, um determinado governo deve classificar, avaliar e priorizar as ameaças de TIC que estão afetando seu território.
- **Etapa 2. Análise do marco:** Com base nos resultados da Etapa 1, os governos devem considerar quais elementos do Marco seriam mais relevantes e aplicáveis à avaliação de ameaças específicas.
- **Etapa 3. Identificação e avaliação de FCC:** Com base na Etapa 2, uma vez que os elementos mais relevantes do Marco tenham sido identificados com base na avaliação nacional de ameaças, os governos podem utilizar a lista das FCC para identificar os recursos específicos necessários para lidar com ameaças específicas. Uma vez concluída essa identificação, pode se tornar-se em uma base útil para avaliar até que ponto um determinado Estado pode tirar proveito do Marco para prevenir ou responder a ameaças específicas.

Essa abordagem é ilustrada usando três cenários: dois que se concentram em diferentes tipos de atos maliciosos (ransomware -sequestro de dados- e negação de serviço distribuída) e um centrado em um vetor específico (manipulação da cadeia de abastecimento).

Independentemente do perfil da ameaça, certos marcos e recursos principais associados devem ser considerados relevantes e aplicáveis independentemente do cenário ou ameaça em consideração, especificamente a Norma A sobre cooperação interestadual e a Norma E sobre direitos humanos. A análise dos três cenários baseia-se neste ponto e identifica elementos específicos de capacidade cibernética adicionais que parecem se repetir em várias ameaças e em várias normas.

A partir de uma perspectiva política e regulatória, os Estados devem priorizar o desenvolvimento (e revisão periódica) de estratégias e políticas nacionais abrangentes de cibersegurança que, em combinação com leis apropriadas, permitam aos Estados tomar todas as medidas necessárias a nível nacional e internacional para garantir a proteção do âmbito das TIC, inclusive através da cooperação com múltiplas partes interessadas. Além disso, os Estados devem priorizar o desenvolvimento de posições públicas e abrangentes sobre como o direito internacional se aplica ao âmbito das TIC.

Do ponto de vista do processo, os Estados devem dar prioridade ao desenvolvimento de mecanismos para facilitar a cooperação em matéria de segurança das TIC com todas as partes interessadas nacionais relevantes, incluindo agências governamentais, o setor privado, a comunidade técnica e a sociedade civil, conforme apropriado. Isso garantiria não apenas fluxos de informações oportunos, eficientes e eficazes em tempos de crise, mas também acesso a ativos de conhecimento que podem ser aproveitados conforme apropriado para compensar possíveis lacunas ou falta de conhecimento

especializado disponível no setor público. Do mesmo modo, os Estados devem desenvolver mecanismos para facilitar a cooperação e a informação a nível bilateral, regional e internacional. O desenvolvimento de processos e mecanismos específicos permitiria a criação de **parcerias e redes funcionais.**

Em relação às estruturas, os Estados devem priorizar o desenvolvimento e a sustentabilidade de **capacidades de resposta a incidentes informáticos nacionais** totalmente operacionais que são elementos insubstituíveis da primeira linha de defesa contra atos maliciosos relacionados às TIC. Vários acordos nacionais e regionais entre CSIRT/CERT públicos e privados poderiam ser explorados para dar conta das limitações de recursos, habilidades ou tecnologias. Além disso, os Estados devem priorizar a identificação de **departamentos responsáveis** dentro do governo nacional para atuar como **pontos focais para questões de TIC nos níveis político e técnico**, inclusive com a criação de um Ponto de Contato Nacional dedicado. A existência de um departamento **com autoridade e poderes para investigar e processar** atos maliciosos relacionados com as TIC parece ser um requisito transversal.

Embora todos os setores sofram de escassez de cibercompetências, a implementação bem-sucedida do Marco dependerá da capacidade dos Estados de desenvolver internamente, ou acederem por meio de parcerias externas, **conhecimentos técnicos e jurídicos** adequados para poder gerir eficazmente incidentes com as TIC com eficácia a nível nacional e garantir a conformidade com o Marco, mas também para se colaborarem de forma construtiva com os seus homólogos a nível internacional em questões relacionadas com a segurança das TIC. Esta também se tornará em uma demanda crescente de diplomatas, que devem reforçar seus conhecimentos sobre as TIC e ser apoiados por especialistas e consultores quando necessário.

Finalmente, a implementação bem-sucedida do Marco também dependerá da capacidade de um Estado de acessar um certo número de **tecnologias e soluções técnicas**, seja desenvolvendo-as em nível nacional ou acessando-as por meio de parcerias com outros (por exemplo, acordos bilaterais ou regionais com outros Estados, ou parcerias público-privadas). Essas soluções de tecnologia incluem, mas não se limitam a, **capacidades para prevenir, detectar e interromper diferentes tipos de ataques** (por exemplo, plataformas de inteligência de ameaças, sistemas de alerta precoce) e soluções para aumentar a confidencialidade, integridade e disponibilidade de sistemas e dados (por exemplo, centros de dados baseados na nuvem).

1. Introdução

As vantagens e oportunidades socioeconômicas oferecidas pelo desenvolvimento rápido e generalizado das tecnologias de informação e comunicação (TICs) trazem novos riscos e ameaças aos Estados-membros e à comunidade internacional em geral. Conforme destacado nos relatórios finais do Grupo de Trabalho de Composição Aberta (OEWG) 2019-2021 sobre desenvolvimentos no campo da informação e telecomunicações no contexto da segurança internacional, e do Grupo de Especialistas Governamentais (GEG) sobre a promoção do comportamento responsável do Estado no ciberespaço no contexto da segurança internacional, os incidentes prejudiciais às TICs estão aumentando em frequência e sofisticação, e estão em constante evolução e diversificação. O primeiro relatório anual de progresso do OEWG 2021-2025 sublinhou igualmente as ameaças crescentes representadas pelas TIC para as infraestruturas e serviços críticos, bem como o risco proveniente de tecnologias novas e emergentes.

Na quarta sessão substantiva do OEWG 2021-2025, realizada em março de 2023, mais de 60 delegações tomaram a palavra para falar sobre o tema das ameaças existentes e potenciais, o maior número de contribuições sobre este tema específico na agenda. A combinação de (1) tensões geopolíticas intensificadas, (2) atividades maliciosas relacionadas às TIC relatadas por atores estatais, (3) incidentes graves de TIC perpetrados por grupos criminosos sofisticados visando serviços públicos e infraestrutura crítica operados pelo setor privado e (4) a maior conscientização sobre o impacto das tecnologias emergentes, como inteligência artificial (IA) e computação quântica, aumentou a profundidade e a amplitude das discussões entre os estados sobre ameaças.

Contudo, a intensidade em que tais discussões estão ligadas ao contexto, escopo e propósito mais amplo do OEWG permanece limitada. À medida que os Estados continuam a discutir os quatro pilares principais do Marco para o Comportamento Responsável do Estado no Uso das TICs (doravante o Marco) - marco de comportamento responsável, direito internacional, medidas de fortalecimento da confiança e capacitação - dois aspectos principais permanecem inexplorados:

a. até que ponto a implementação do Marco pode ser usada para aumentar a segurança nacional, regional e internacional e a resiliência contra ameaças específicas; e
b. como ameaças específicas podem ser usadas para informar iniciativas de capacitação.

Este relatório é o segundo de um estudo de duas partes realizado pelo UNIDIR que visa fortalecer os vínculos entre o Marco e a capacidade dos Estados de prevenir ou mitigar efetivamente o impacto de atividades maliciosas relacionadas às TIC, concebendo uma ferramenta para melhor identificar os requisitos e priorizar intervenções para reforço das capacidades.

Este relatório se concentra no conceito de Capacidades Cibernéticas Fundamentais (FCC) conforme apresentado e descrito no primeiro relatório deste estudo.[1]

1 Consulte Samuele Dominioni e Giacomo Persi Paoli. 2023. Descobrindo as necessidades de desenvolvimento de habilidades cibernéticas: Parte I. Classificando as habilidades cibernéticas fundamentais. JUNTAR.

2. Resumo dos Principais Conceitos

2.1 O Marco de Ação para o Comportamento do Estado Responsável no uso das TIC

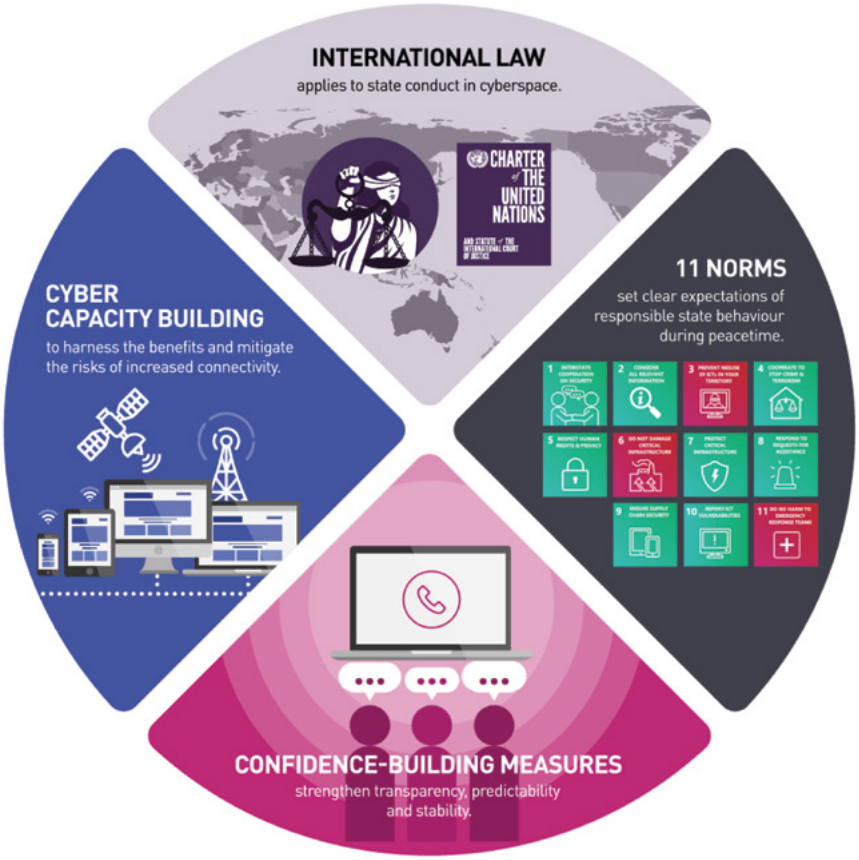
Nas últimas duas últimas décadas, os Estados-membros têm discutido o uso das TIC no contexto da paz e segurança internacional. Após o GEG de 2015, a Assembleia Geral desenvolveu e adotou um conjunto de 11 normas voluntários não vinculativas de comportamento responsável do Estado[2] e aperfeiçoou-as em processos multilaterais subsequentes.[3] Estas normas, combinados com a

2 Ver A/RES/70/237.

3 Ver Relatório substantivo final do OEWG 2021, e Relatório GEG 2021.

reafirmação de que o direito internacional é aplicável ao âmbito das TIC, com medidas dedicadas ao fortalecimento da confiança (CBM por suas siglas em inglês) e iniciativas específicas de criação de capacidades e cooperação, constituem os elementos do Marco para Comportamento Responsável do Estado no Ciberespaço (ver figura 1).

Figura1. Marco das Nações Unidas para o Comportamento Responsável do Estado no Ciberespaço



Fonte: https://www.internationalcybertech.gov.au/un-cyber-norms-resources

Um componente chave do Marco são as 11 normas voluntárias. Estas abordam uma vasta gama de questões internacionais de cibersegurança e indicam os comportamentos que os Estados devem e não devem adotar no uso das TIC para preservar a paz e a segurança no âmbito das TIC. A Tabela 1 fornece uma visão geral das 11 normas.

Tabela 1. Normas de Conduta para o Comportamento Responsável do Estado no Ciberespaço[4]

	**Norma A** De acordo com os propósitos das Nações Unidas, incluindo a manutenção da paz e segurança internacionais, os Estados devem cooperar no desenvolvimento e implementação de medidas para aumentar a estabilidade e segurança no uso das TIC e prevenir práticas de TIC que são reconhecidas como prejudiciais ou que possam representar ameaças à paz e segurança internacionais.
	**Norma B** No caso de incidentes de TIC, os Estados devem considerar todas as informações relevantes, incluindo o contexto mais amplo do evento, desafios de atribuição no ambiente das TIC e a natureza e extensão das consequências.
	**Norma C** Os Estados não devem permitir conscientemente que seu território seja usado para atos internacionalmente ilícitos usando as TIC.
	**Norma D** Os Estados devem considerar a melhor forma de cooperar para trocar informações, prestarem assistência mútua, processar o uso terrorista e criminoso das TIC e implementar outras medidas de cooperação para lidar com tais ameaças. Os Estados poderão ter de considerar se é necessário desenvolver novas medidas a esse respeito.
	**Norma E** Os Estados, ao garantir o uso seguro das TIC, devem respeitar as resoluções 20/8 e 26/13 do Conselho de Direitos Humanos sobre a promoção, proteção e gozo dos direitos humanos na Internet, bem como as resoluções 68 /167 e 69/166 da Assembleia Geral sobre o direito à privacidade na era digital, para garantir o pleno respeito aos direitos humanos, incluindo o direito à liberdade de expressão.

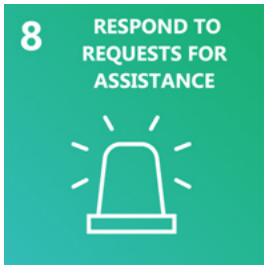
4 Ícones de: https://www.internationalcybertech.gov.au/un-cyber-norms-resources.

Norma F

Um Estado não deve realizar ou apoiar conscientemente uma atividade de TIC contrária às suas obrigações ao abrigo do direito internacional que danifique intencionalmente a infraestrutura crítica ou de outra forma prejudique o uso e a operação da infraestrutura crítica para prestar serviços ao público.

Norma G

Os Estados devem tomar as medidas apropriadas para proteger sua infraestrutura crítica contra ameaças relacionadas às TIC, levando em consideração a resolução 58/199 da Assembleia Geral.



Norma H

Os Estados devem responder às solicitações apropriadas de assistência de outro Estado cuja infraestrutura crítica esteja sujeita a atos maliciosos de TIC. Os Estados também devem responder às solicitações apropriadas para mitigar atividades maliciosas relacionadas às TIC direcionadas à infraestrutura crítica de outro Estado e originárias de seu território, com o devido respeito por sua soberania.

Norma I

Os Estados devem tomar medidas razoáveis para garantir a integridade da cadeia de abastecimento para que os usuários finais possam confiar na segurança dos produtos de TIC. Os Estados devem tentar prevenir a proliferação de ferramentas e técnicas de TIC maliciosas e o uso de funções ocultas nocivas.

Norma J

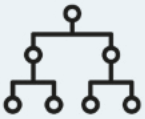
Os Estados devem encorajar o relato responsável de vulnerabilidades de TIC e compartilhar informações associadas sobre soluções disponíveis para tais vulnerabilidades, a fim de limitar e possivelmente eliminar ameaças potenciais às TIC e à infraestrutura dependente de TIC.

Norma K

Os Estados não devem conduzir ou apoiar conscientemente atividades que danifiquem os sistemas de informação das equipes autorizadas de resposta a emergências (às vezes conhecidas como equipes de resposta a emergências informáticas ou equipes de resposta a incidentes de cibersegurança) de outro Estado. Um Estado não deve usar equipes de resposta a emergências autorizadas para se envolver em atividades internacionais maliciosas.

2.2 Capacidades Cibernéticas Fundamentais[5]

Capacidades Cibernéticas Fundamentais (FCC), são definidos como a combinação de políticas e regulamentos, processos e estruturas, alianças e redes, pessoas e habilidades e tecnologia necessária para implementar o Marco. Para efeitos deste estudo, estes cinco pilares são definidos da seguinte forma:

Políticas e Regulamentos 	Documentos oficiais relacionados a questões de cibersegurança. Estes incluem documentos que descrevem as posições, políticas e estratégias (desenvolvidas especificamente para setores-chave, por exemplo, infraestrutura crítica ou para aplicações intersetoriais a nível nacional) dos Estados-membros, bem como marcos legais e regulatórios e assinatura de acordos ou outras formas de cooperação com partes interessadas internacionais.
Processos e Estruturas 	Cargos-chave, agências/entidades responsáveis, outros mecanismos nacionais ou regionais e processos, procedimentos e protocolos oficiais relacionados com a cibersegurança.
Alianças e Redes 	Iniciativas, tanto a nível nacional como internacional destinadas a fortalecer as capacidades nacionais. A nível nacional, inclui mecanismos ou instrumentos de cooperação intrassetorial e intragovernamental. A nível internacional, mecanismos ou instrumentos de cooperação bilateral, regional e multilateral.
Pessoas e Habilidades 	Conhecimento e experiência especializada em cibersegurança. Note-se que algumas FCC listados no pilar “pessoas e competências” poderão também ser cumpridos através da terceirização e do estabelecimento de acordos com provedores externos ou outras partes interessadas quando o Estado não puder desenvolver ou manter internamente as capacidades especializadas.

5 Esta seção é um trecho da primeira parte deste estudo apresentado em Samuele Dominioni e Giacomo Persi Paoli. 2023. Descobrindo as necessidades de desenvolvimento de habilidades cibernéticas: Parte I. Classificando as habilidades cibernéticas fundamentais. UNIDIR.

Tecnologia 	Soluções/capacidades técnicas a nível nacional relacionadas com a cibersegurança. Deve-se notar que as FCC listados no pilar 'tecnologia' também podem ser atendidos por terceirização para provedores de serviços externos por meio, por exemplo, de parcerias público-privadas.

A lista da FCC não pretende ser representativa das melhores práticas ou medidas desejáveis. **Foi desenvolvida com a ideia de servir de base para o desenvolvimento de respostas mais refinadas e abrangentes,** uma vez que essa base seja alcançada. Portanto, os FCC representam os **requisitos mínimos de capacidade necessários para a implementação do Marco**, não soluções ótimas ou respostas ideais. Como tal, os elementos que não emergiram como verdadeiramente necessários ou fundamentais, mas mais aspiracionais, desejáveis ou "avançados", não foram incluídos na lista. Além disso, também é importante observar que a ênfase está em qual capacidade deve estar presente e não em como desenvolvê-la, o que continua sendo uma prerrogativa nacional.[6] O Anexo A contém a lista completa das FCC para cada elemento do Marco e o primeiro relatório do presente estudo explica mais pormenorizadamente sobre cada FCC.

6 Samuele Dominioni e Giacomo Persi Paoli. 2023. Descobrindo as necessidades de desenvolvimento de habilidades cibernéticas: Parte I. Classificando as habilidades cibernéticas fundamentais. UNIDIR.

3. Introdução à Abordagem Baseada em Ameaças

Conforme mencionado no Capítulo 1, o cenário de ameaças no âmbito das TIC está em constante evolução, torna-se mais complexo e sofisticado à medida que a base de referência das medidas de cibersegurança é cada vez maior. Embora se deva observar que mais de noventa por cento dos ataques cibernéticos poderiam ser evitados[7] através da aplicação sistemática de medidas básicas de "higiene" de segurança (por exemplo, alterar senhas padrão predefinidas, utilizar autenticação de multifator, usar anti-malware, instalar atualizações de segurança oportunamente etc.), o Marco para Comportamento Responsável do Governo pode fornecer uma camada adicional importante para a resiliência. De fato, a criação de capacidades necessárias para implementar o Marco equiparia os Estados com ferramentas importantes que podem contribuir para prevenir ou mitigar ciberameaças específicas, bem como para fortalecer sua ciber-resiliência global.

---

7 Existem diferentes estimativas de várias empresas de cibersegurança e tecnologia. Por exemplo, o Relatório de Defesa Digital da Microsoft publicado em novembro de 2022 estima que a higiene básica de segurança ainda protege contra 98% dos ataques; ver https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.

Na última década, foram desenvolvidas e aplicadas com êxito várias metodologias, modelos e abordagens para identificar quais elementos e medidas os governos devem adotar para desenvolver ou fortalecer suas capacidades nacionais de TIC.[8] No entanto, nenhum modelo existente aborda especificamente a implementação do Marco considerando diferentes contextos nacionais e diferentes percepções das ameaças.

Neste contexto, este projeto de investigação propõe uma abordagem que permitiria aos governos avaliar melhor sua preparação para aproveitar o Marco para prevenir ou responder a atividades maliciosas e ameaças específicas das TIC. A proposta de "abordagem baseada em ameaças" compreende três etapas:

- **Etapa 1. Avaliação de ameaças e riscos**: Nesta etapa, um determinado governo deve classificar, avaliar e priorizar as ameaças de TIC que estão afetando seu território. Ao efetuar esta análise, os governos podem basear-se em fontes nacionais (por exemplo, relatórios de inteligência de ameaças de suas agências/entidades de cibersegurança) e/ou outras fontes (por exemplo, relatórios de inteligência de ameaças fornecidos por empresas privadas). Deve-se também levar em consideração não só o tipo de ataque ou malware utilizado, mas também elementos mais amplos, como os alvos mais vulneráveis ou expostos, os diferentes tipos de agentes de ameaças, a possível natureza transfronteiriça da própria ameaça ou das possíveis respostas entre outros. É importante que essas avaliações de ameaças também considerem cenários de risco em que o país não é necessariamente a vítima pretendida do ataque, mas talvez sirva como vítima instrumental, por exemplo, como país de "trânsito" ou rota para um ataque destinado a outra pessoa. Um exemplo de uma ferramenta que os governos podem utilizar para efetuar uma avaliação exaustiva das ameaças e dos riscos é a Taxonomia de Incidentes Maliciosos nas TIC do UNIDIR.[9]
- **Etapa 2. Análise do marco**: Com base nos resultados da Etapa 1, os governos devem considerar quais elementos do Marco seriam mais relevantes e aplicáveis à avaliação de ameaças específicas. É importante reconhecer que cada ameaça ou incidente de TIC, mesmo do mesmo tipo, embora tenha certas semelhanças, também será caracterizado por fatores únicos. No entanto, ao analisar perfis de ameaças mais gerais, em vez de incidentes específicos e únicos, pode ser possível identificar quais normas, elementos do direito internacional e medidas de fortalecimento da confiança seriam mais relevantes.
- **Etapa 3. Identificação e avaliação das FCC:** Com base na Etapa 2, uma vez que os elementos mais relevantes do Marco tenham sido identificados com base na avaliação nacional de ameaças, os governos podem usar a lista da FCC (consulte o Anexo A) para identificar as capacidades necessárias para lidar com ameaças específicas. Se todas as FCC listadas em cada elemento do Marco ou apenas uma seleção delas seriam aplicáveis, dependeria da ameaça específica em

8 Refira-se ao **Oxford Cybersecurity Capability Maturity Model for Nations (CMM)** e à **Pesquisa do Índice Global de Cibersegurança da União Internacional de Telecomunicações**.

9 Samuele Dominioni e Giacomo Persi Paoli. 2022. Uma taxonomia de incidentes maliciosos de TIC. UNIDIR. **https://unidir.org/publication/taxonomy-malicious-ict-incidents**.

questão. Uma vez concluída essa identificação, ela pode se tornar uma linha de base útil para avaliar até que ponto um determinado Estado pode aproveitar o Marco para prevenir ou responder a ciberameaças específicas.

Para além de informar as prioridades de capacidades ao fornecer outra perspectiva sobre possíveis lacunas e necessidades, essa metodologia também oferece dois benefícios adicionais. Primeiro, os governos poderiam utilizá-lo para realizar "verificações de integridade" regulares em suas arquiteturas de cibersegurança, a fim de garantir que estas se mantêm adequadas à evolução das ameaças. Em segundo lugar, poderia ser usado para realizar exercícios teóricos regulares baseados em cenários (nacional ou regional) envolvendo todas as partes interessadas relevantes para examinar a preparação e resiliência para prevenir ou gerir ameaças novas e existentes.

Deve-se notar que esta abordagem não tenta classificar os componentes do Marco, ou mesmo as próprias normas, por importância. Todos os componentes do Marco são essenciais e devem ser levados em consideração. No entanto, ao analisar cenários de ameaças específicos, diferentes capacidades podem ser mais relevantes ou aplicáveis do que outros para lidar com circunstâncias específicas. Algumas capacidades podem até ser um pré-requisito para outras.

Por fim, é importante observar que fatores além da lista da FCC, que foi desenvolvida exclusivamente com foco no Marco, acabarão afetando a capacidade de um Estado de prevenir ou mitigar ameaças cibernéticas. No entanto, conforme mencionado anteriormente nesta seção, desenvolver ou fortalecer as capacidades para implementar o Marco contribuirá positivamente para a resiliência cibernética geral de um Estado.

4. A Abordagem Baseada em Ameaças em Ação: Exemplos Ilustrativos

Para desenvolver a abordagem baseada em ameaças e ilustrar como pode ser utilizada para identificar requisitos de capacidade específicos, a equipe do projeto desenvolveu três cenários de ameaças diferentes e os utilizou para realizar workshops sobre o tema com especialistas internos e externos.[10] Com base na análise das discussões mais recentes sobre ameaças existentes e emergentes no

10 Workshops de especialistas externos e internos alternaram sessões plenárias e grupos de trabalho para analisar, apoiados por cenários dedicados, os três estudos de caso com o objetivo de classificar elementos relevantes do Marco para FCC específicos e necessidades de desenvolvimento de capacidades relacionadas. Por exemplo, usando ransomware como ponto de entrada, os participantes do workshop revisaram o Marco para identificar normas relevantes, elementos do direito internacional ou medidas de fortalecimento da confiança que podem ser aplicadas ao cenário. Em seguida, selecionaram os elementos da FCC mais adequados para lidar com a ameaça. Os dados dessas duas oficinas foram agregados e analisados. Durante um evento paralelo na quarta sessão do OEWG em Nova York (6 a 10 de março de 2023), a UNIDIR apresentou os resultados preliminares do projeto de investigação. Posteriormente, foram realizadas verificações adicionais das constatações com especialistas externos.

contexto do OEWG, três ameaças cibernéticas específicas foram selecionadas como exemplos ilustrativos para esta metodologia: duas focadas em diferentes tipos de atos maliciosos (malware e negação de serviço distribuída) e um centrado em um vetor específico[11] (manipulação da cadeia de abastecimento). Em particular, os atos maliciosos relacionados às TIC propostos para este estudo são os seguintes.

a. **Operações de malware direcionadas a dados** (por exemplo, ransomware, limpadores de dados): software malicioso que visa comprometer a confidencialidade, integridade ou disponibilidade dos dados. Ransomware é um tipo de malware que procura criptografar dados ou ameaça divulgar dados exfiltrados para obter o pagamento de um resgate. Um limpador é uma classe de malware destinada a apagar ("wipe", daí o nome) o disco rígido do computador que infecta, removendo maliciosamente dados e programas.
b. **Lei de Negação de Serviço Distribuída (DDOS)** – Um tipo de operação cibernética em que um ator mal-intencionado visa tornar um computador, dispositivo ou rede indisponível interrompendo a operação normal do dispositivo sobrecarregando-o com solicitações do sistema até que o tráfego normal não possa ser processado, resultando em uma negação de serviço.
c. **Manipulação da cadeia de abastecimento de software**: Um ato que injeta código malicioso em um aplicativo ou software para infectar todos os usuários. Ao manipular a cadeia de fornecimento de software, os atores mal-intencionados buscam tirar proveito das relações de confiança entre clientes e provedores, que podem não saber que seu software está infectado com código malicioso quando o liberam para o público. O código malicioso é executado com a mesma confiança e permissões do software original ao qual está anexado.

Além da natureza específica do ato malicioso, os três cenários de ameaça incluem variações de outros fatores-chave: **tipos de vítimas** (por exemplo, operadores de infraestrutura crítica, agências governamentais, outros atores e usuários do setor privado), incerteza sobre a **participação do estado como perpetrador e dimensões transfronteiriças** do incidente. Não há uma lista padrão ou recomendada de fatores a serem considerados ao pensar em ameaças. A taxonomia do UNIDIR de incidentes maliciosos de TIC oferece uma boa visão geral do que esses fatores podem ser, mas é uma escolha que depende de contextos nacionais ou regionais.

Para adicionar mais realismo ao exercício e estimular discussões mais focadas, os três perfis de ameaças foram desenvolvidos em narrativas curtas de cenários, baseadas em eventos reais, que foram usadas para descrever um incidente cibernético específico (embora hipotético).
Deve-se notar que, independentemente das ameaças, alguns elementos do Marco e as capacidades associadas devem ser consideradas como sendo sempre igualmente aplicáveis. Estas são a Norma A e a Norma E:

11 "Vetor" refere-se ao método de invasão em um sistema ou rede; ver Samuele Dominioni e Giacomo Persi Paoli. 2022. Uma taxonomia de incidentes maliciosos de TIC. JUNTAR. https://unidir.org/publication/taxonomy-malicious-ict-incidents.

	**Norma A**
	Esta norma é sempre aplicável dado o seu carácter estratégico/de alto nível que suporta qualquer forma de cooperação entre Estados em matéria de segurança internacional das TIC e a sua implementação inclui elementos fundamentais, como Equipes de Resposta a Incidentes de Segurança Informática (CSIRT) / Equipes de Resposta a Emergências Informáticas (CERT), que são fundamentais para garantir a resiliência cibernética nacional.
	**Norma E**
	Esta norma é sempre aplicável uma vez que o respeito pelos direitos humanos está subjacente ao comportamento dos Estados no âmbito das TIC, independentemente do cenário de ameaça.

Por último, vale a pena notar que vários FCC se repetem em vários cenários, às vezes com nuances mais específicas, às vezes como requisitos idênticos. Isto se deve ao fato de que cada cenário deve ser lido como uma seção separada e, portanto, todas as informações relevantes são fornecidas.

4.1 Cenário 1: Ransomware

Perfil de Ameaça

Tipo	Ransomware
Vítima	Duas infraestruturas críticas no setor energético
Autor	Grupo criminoso com possível envolvimento de um ator estatal
Transfronteiriço	Sim; as sedes das infraestruturas estão localizadas em dois países diferentes, e as evidências apontam para o envolvimento de dois criminosos diferentes, ambos sediados em países terceiros

Descrição do Cenário

Neste cenário, os criminosos usaram ransomware para realizar um ato malicioso relacionado às TIC visando duas infraestruturas críticas transnacionais na indústria de petróleo e gás, com sede em dois países diferentes (país Alfa e país Beta). Este ato levou a uma redução de sessenta por cento na distribuição de petróleo e gás no país Alfa. A nota de resgate exigia o pagamento de US$ 10 milhões. A análise preliminar de empresas de cibersegurança sugeriu que o ato foi lançado por um grupo de hackers criminosos que opera principalmente em um terceiro país (país Charlie). Subsequentemente, análises forenses adicionais da unidade de aplicação da lei de cibersegurança do país Alfa descobriram que o malware exibia um nível de sofisticação e alguns marcadores específicos associados às capacidades cibernéticas, táticas, técnicas e procedimentos de outro país, país Zero, embora nenhuma evidência conclusiva tenha sido encontrada. O país Alfa e o país Zero têm um histórico de relações diplomáticas difíceis devido a interesses geoestratégicos conflitantes.

Elementos do Marco Relevantes para o Cenário

Com base em pesquisas e consultas a especialistas, os seguintes componentes do Marco foram considerados particularmente relevantes para este cenário:

Norma B

Dada a complexidade do cenário, a incerteza sobre o perpetrador e possível envolvimento do país Zero e o contexto geopolítico mais amplo, a Norma B é particularmente relevante para ambos os Estados vítimas (Alfa e Beta) que podem querer atribuir o ataque a um ator específico.

Norma C

No cenário, as evidências iniciais sugerem que o perpetrador, um grupo criminoso de hackers, estava operando no país Charlie. Como tal, a Norma C torna-se altamente relevante para o país Charlie, que deve agir de acordo com esta regra.

Norma D

Para poder tomar medidas em resposta às informações disponíveis que apontam para o possível envolvimento de um grupo criminoso baseado no país Charlie, é importante que os países-alvo (Alpha e Beta) e país Charlie estejam equipados com as capacidades necessárias para implementar a Norma D a fim de cooperar.

Norma F

Dado o alvo desse ataque e o possível papel desempenhado pelos países Charlie e Zero, a regra F também é altamente relevante.

Norma G

Espelhando a consideração feita para a Norma F, a Norma G torna-se altamente relevante para os países Alfa e Beta cuja infraestrutura crítica foi atacada.

Medidas de Construção de Confiança

Dada a dimensão transnacional dos incidentes e a possível participação de outros dois países, a capacidade de implementar as CBM que apoiem a comunicação e a transparência entre os Estados é particularmente relevante.

Lei Internacional

A maioria dos regulamentos considerados relevantes para este cenário requer para sua implementação a formulação de interpretações nacionais claras de conceitos legais (por exemplo, devida diligência, infraestrutura crítica, princípio da não intervenção).

FCC Relevantes Aplicáveis ao Cenário

Políticas e Regulamentos	• Em relação às **políticas e regulamentações** relevantes para este cenário, todos os países envolvidos devem ter desenvolvido uma **interpretação nacional de todas as normas em questão e sua compreensão de como o direito internacional (DI) se aplica ao âmbito das TIC**. • O país Alfa deve ter uma política que descreva a **metodologia e as definições para sua atribuição.** • Dadas as diferentes partes interessadas envolvidas no incidente, os **marcos que permitem o compartilhamento de informações** com as partes interessadas comerciais e não governamentais relevantes são particularmente importantes (Normas D, G). • Tendo em conta o papel de um grupo criminoso no cenário, os países envolvidos nos incidentes devem ter **estratégias, políticas e legislação adequadas que estabeleçam disposições para prevenir, detectar e interromper o uso malicioso das TIC** (Norma C) e que **permitam a cooperação** na investigação e repressão de atividades cibercriminosas (Norma D). Dada a natureza específica do ataque, essas políticas e estratégias também devem abranger a **segurança dos dados** para garantir que medidas apropriadas possam ser implementadas para criar cópias de segurança e redundâncias. • Os países Alfa e Beta (países-alvo) deveriam ter **setores de infraestrutura crítica e aprovado legislação sobre a proteção de infraestrutura crítica** (Norma G). • Finalmente, os governos dos países Charlie e Zero deveriam ser capazes de demonstrar que suas **políticas e legislações nacionais estão alinhadas com a Norma F** e com o requisito de não danificar a infraestrutura crítica. No mínimo, **seria necessária uma interpretação pública adequada do padrão.**
Processos e Estruturas	• Os países Alfa e Beta, como países-alvo, devem desenvolver **normas nacionais de comprovação de atribuição** (Norma B), bem como processos e procedimentos que permitam o **compartilhamento de informações e a cooperação entre entidades governamentais e não governamentais relevantes** em todos os países envolvidos, incluindo protocolos especialmente para evidências digitais (Normas A, B, C, D, G). • Em termos de estruturas, os países devem ter **CSIRT/CERT nacionais ou regionais** bem estabelecidos e em pleno funcionamento (Norma A, C, D, G, CBM), bem como **Pontos de Contato a nível diplomático e técnico** (Norma A, CBM) e um **mecanismo de supervisão independente e eficaz**, capaz de garantir a transparência e a responsabilização pela operação do Estado (incluindo a coleta de dados) no âmbito das TIC (Norma A, E, F e DI).

Alianças e Redes	• Nos países-alvo, a cooperação intersetorial, inclusive com o setor privado, seria fundamental para resolver e recuperar-se adequadamente dos atos maliciosos das TIC (Norma A). Tal deve incluir **cooperação transfronteiriça com proprietários e operadores de infraestrutura relevantes** (Norma G). • Entre os países-alvo, a **cooperação bilateral seria essencial para garantir o compartilhamento de informações** (no âmbito das Normas A, B, C e F) e investigações transfronteiriças (Norma D). • A **cooperação bilateral** também seria importante entre os países-alvo (Alfa e Beta) e os países potencialmente envolvidos no ato malicioso (Charlie e Zero) com especial ênfase na resolução de **divergências e disputas** (conforme as Norma B) e na investigação (sob a Norma D).
Pessoas e Habilidades	• Para responder adequadamente ao cenário, países Alfa e Beta específicos necessitaria de especialistas com habilidades em **gestão de incidentes de cibersegurança** (Norma A), bem como na **condução ou avaliação de investigações técnicas** de incidentes de TIC (Norma B). O país Charlie também necessitaria de especialistas para **identificar e interromper atos maliciosos nas TIC** provenientes de seu próprio território (Norma C). • Além das habilidades técnicas e de gestão de incidentes, é importante que todos os governos envolvidos tenham acesso a **conhecimentos jurídicos** sobre a aplicabilidade do direito internacional no contexto das TIC (Normas A, B, F e DI), bem como **habilidades diplomáticas e comunicação pública** específicas para o contexto das TIC e infraestruturas críticas (Normas B, C, G e CBM).
Tecnologia	• Dependendo do cenário, os países-alvo e o país a partir do qual o grupo cibercriminoso suspeito opera devem estar equipados com **capacidades técnicas para prevenir, detectar e interromper atos maliciosos das TIC**, particularmente contra infraestrutura crítica (Normas A, C, D, G). Os países-alvo do ransomware também necessitarão de soluções tecnológicas para garantir a cópia e redundância dos dados (por exemplo, centros de dados baseados. na nuvem).

4.2. Cenário 2: Negação de Serviço Distribuído (DDoS)

Perfil de Ameaça

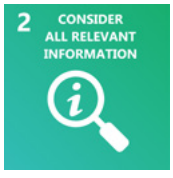
Tipo	Negação de Serviço Distribuído (DDO)
Vítima	Sites e aplicativos do governo
Autor	Uma Ameaça Persistente Avançada (APT) com envolvimento plausível de um ator estatal
Transfronteiriço	Sim; ataques foram encaminhados através de vários países

Descrição do Cenário

O país Alfa sofreu uma campanha prolongada de múltiplos ataques DDoS direcionados a seus serviços públicos (incluindo sistemas de previdência social). As primeiras investigações dos incidentes destacaram que atos maliciosos foram canalizados através de computadores e redes em dois outros países (Beta, Charlie). À medida que os ataques DDoS aumentavam em frequência e magnitude, o país Alfa declarou estado de emergência. Investigações adicionais levadas a cabo pelas autoridades do país Alfa relacionaram os atos maliciosos relacionados às TIC a uma conhecida APT estreitamente associada ao governo de terceiro país com interesses estratégicos concorrentes (país Zero).

Elementos do Marco Relevantes para o Cenário

Com base em investigações e consultas a especialistas, os seguintes componentes do Marco foram considerados particularmente relevantes para este cenário:



Norma B

Neste cenário, a combinação do encaminhamento dos ataques através países terceiros, a eventual participação de uma APT associada a outro Estado e a gravidade do impacto que levou à declaração de emergência nacional, pode levar à vítima (país Alfa) a considerar a opção de atribuir publicamente o ataque a outro Estado. Neste caso, a Norma B é particularmente relevante.

Norma C

Esta regra é particularmente relevante para os “países de trânsito' neste cenário que desempenham um papel fundamental na interrupção do ataque.

Norma D

Para responder eficazmente a este cenário de ameaças, o país vítima e os países de trânsito devem ser capazes de implementar de forma eficaz a norma que insta à cooperação para impedir as atividades maliciosas perpetradas pela APT.

Medidas de Construção de Confiança

Dada a dimensão transnacional dos incidentes, a implementação efetiva da CBM, em especial Pontos de Contato bem estabelecidos e totalmente operacionais nos níveis diplomático e técnico, seria particularmente relevante para gerir as respostas operacionais e políticas ao incidente.

Lei Internacional

O cenário de ameaças apresentado neste caso, juntamente com as normas destacadas como relevantes, exige que os países envolvidos desenvolvam posições claras sobre questões fundamentais do direito internacional, como a devida diligência, o princípio da não intervenção e o princípio da responsabilidade do Estado.

FCC Relevantes Aplicáveis ao Cenário

Políticas e Regulamentos

- Em relação às políticas e regulamentos, como ponto de partida, os países devem ter **interpretações nacionais dos componentes do Marco aplicáveis a este cenário** (Normas B, C, D e DI). Isto fornecerá a base sobre a qual construir a resposta específica.
- Além disso, existem várias políticas e regulamentos que os países deveriam ter adotado/implementado em função do seu papel no cenário. Relativamente à Norma B sobre atribuição, o país Alfa, como país vítima, deve ter uma **classificação de incidente de TIC em termos de escala e impacto** que possa sustentar uma declaração de estado de emergência e uma política de atribuição, incluindo definições e metodologia.
- A norma C é particularmente relevante para os países de trânsito, que devem ter **políticas e estratégias de cibersegurança que definam disposições para prevenir, detectar e interromper atos maliciosos de TIC**, apoiados por **medidas legislativas apropriadas para investigar e processar** tais atos (Norma C e D).
- Todos os países envolvidos devem também ter estabelecido **regulamentos que permitam a cooperação e compartilhamento de informações** com entidades comerciais e não governamentais relevantes (Norma D).

Processos e Estruturas	• Existem vários processos e estruturas relevantes para este cenário. Em termos de processos, para apoiar a possível atribuição do incidente a um país terceiro (Norma B), o país Alpha deve desenvolver **normas nacionais de evidência, e processos e procedimentos** (incluindo protocolos em especial para o compartilhamento de evidências digitais) **com o objetivo possibilitar o compartilhamento de informações** entre entidades governamentais e não governamentais relevantes (Normas B, C e D). • Em termos de estruturas, os países deveriam ter **CSIRT/CERT nacionais ou regionais** (Normas A, C, D). • Dada a dimensão transnacional dos ataques DDoS, é também indispensável que os países Alpha, Beta e Charlie tenham **capacidades de aplicação da lei cibernética** (Normas C, D), bem como **mecanismos de cooperação** entre eles (Norma A) para intervir rápida e eficazmente as atividades maliciosas. • Os **Pontos de Contato Nacionais** ao nível diplomático e técnico (Norma A, CBM) desempenhariam um papel fundamental na gestão e resolução do incidente. • Finalmente, todos os Estados envolvidos devem ter um **mecanismo de supervisão independente e eficaz**, capaz de garantir a transparência e a responsabilidade pela operação do Estado (incluindo a coleta de dados) no âmbito das TIC (Normas A, E e DI).
Alianças e Redes	• Para gerir um ataque global às instituições públicas, é necessária a **cooperação intragovernamental e a cooperação de várias partes interessadas** (Normas A, C). • A **cooperação internacional** centrada no **compartilhamento de informações** (Normas A, B, C) **e investigação e ação penal** (Norma D) entre os países Alfa, Beta e Charlie seria essencial e exigiria a disponibilidade de **protocolos e mecanismos de cooperação**. • Ao mesmo tempo, é crucial que a **cooperação e comunicação bilateral,** através dos **Pontos de Contato** e canais diplomáticos entre o país Alfa e o país Zero, seja necessária para gerir as implicações políticas do incidente e trabalhar no sentido de resolver divergências e disputas.

Pessoas e Habilidades	• Para responder adequadamente ao cenário, o país-alvo Alfa necessitaria de especialistas com habilidades para a **gestão de incidentes de cibersegurança** (Norma A) e para **conduzir ou avaliar investigações técnicas** de incidentes de TIC em apoio à implementação do Norma B. Os países Beta e Charlie também precisariam de conhecimentos especializados para **identificar e interromper atos maliciosos das TIC** provenientes de seu próprio território (Norma C). • Além das habilidades técnicas e de gestão de incidentes, é importante que todos os países envolvidos tenham acesso a **conhecimentos jurídicos** sobre a aplicabilidade do direito internacional no contexto das TIC (Normas A, B, F e DI), bem como **habilidades diplomáticas e comunicação pública** específica para o contexto das TIC para gerir eficazmente as relações bilaterais com outros países envolvidos e a comunicação pública mais geral com outros países e partes interessadas (Normas B, C, G e CBM).
Tecnologia	• Os elementos tecnológicos relacionados a este cenário referem-se a **capacidades para prevenir, detectar e interromper ataques DDoS** no país vítima e nos países de trânsito. Isso pode incluir, por exemplo, soluções de rede de entrega de conteúdo para ajudar a absorver e desviar um ataque DDoS, distribuindo o tráfego em vários servidores para mitigar o impacto de um ataque e evitar um único ponto de falha, ou proteção DDoS baseada na nuvem para detectar e mitigar ataques em tempo real, aproveitando a escalabilidade da nuvem para lidar com ataques em larga escala.

4.3. Cenário 3: Manipulação da Cadeia de Abastecimentos

Perfil de Ameaça

Tipo	Malware (porta traseira da cadeia de abastecimento)
Vítima	Um fornecedor de software de cibersegurança e milhares de usuários, incluindo instituições públicas
Autor	Ator estatal desconhecido, mas plausível
Transfronteiriço	Sim; as vítimas estão espalhadas por todo o mundo e a invasão foi roteada por meio de servidores em vários países

Descrição do Cenário

Uma empresa de cibersegurança com sede no país Alfa descobriu um malware que tinha infectado um grande número de sistemas de clientes. O malware parecia ter sido distribuído por meio de um ato de manipulação da cadeia de abastecimento visando um fornecedor de software terceirizado (sediado no mesmo país) que inadvertidamente distribuiu o malware backdoor através de uma atualização de software programada. Mais de 50.000 organizações públicas e privadas em todo o mundo utilizam o software em questão como ferramenta de gestão empresarial. Como resultado, o ataque comprometeu dados, redes e sistemas de milhares de organizações e usuários e expôs potencialmente seus clientes e parceiros. A análise efetuada pelas autoridades de vários países sugeriu que, ao gerir a intrusão em vários servidores localizados em diferentes países e ao imitar o tráfego de rede legítimo, os criminosos conseguiram contornar as técnicas de detecção de ameaças utilizadas por empresas privadas e agências governamentais, o que denota um nível de sofisticação próprio de um ator estatal avançado.

Elementos do Marco Relevantes para o Cenário

Com base em investigações e consultas a especialistas, os seguintes componentes do Marco foram considerados particularmente relevantes para este cenário:

	**Norma D**
	O malware tinha como alvo um fornecedor de software no país Alpha, mas o impacto foi global, exigindo cooperação entre Estados na investigação e repressão do incidente.
	**Norma G**
	Dada a escala e o impacto do ato malicioso, é essencial garantir que a infraestrutura crítica seja protegida contra os riscos da cadeia de abastecimentos.

Norma I

Como o cenário é baseado em uma cadeia de abastecimentos de software comprometida, esta norma é crítica para o cenário.

Medidas de Construção de Confiança

Tendo em conta a dimensão transnacional dos incidentes, são particularmente relevantes as medidas de reforço da confiança com o objetivo de apoiar uma comunicação e compartilhamento de informações mais eficientes entre os Estados.

Lei Internacional

Apesar da falta de evidências suficientes para atribuir o ataque a um perpetrador específico, o cenário de ameaça apresentado neste caso, juntamente com as normas destacadas como relevantes, exige que os Estados envolvidos desenvolvam posições claras sobre questões fundamentais do direito internacional, como a devida diligência (particularmente no país Alfa), o princípio da não intervenção e o princípio da responsabilidade do Estado.

FCC Relevantes Aplicáveis ao Cenário

Políticas e Regulamentos

- Todos os países envolvidos no incidente deveriam ter adotado e implementado **políticas e estratégias para prevenir, detectar e interromper atos maliciosos relacionados às TIC**, apoiados por **medidas legislativas apropriadas para investigar e processar** tais atos (Norma D).
- Todos os países envolvidos também deveriam ter estabelecido **regulamentos que permitam a cooperação e compartilhamento de informações** com entidades comerciais e não governamentais relevantes (Norma D).
- Para salvaguardar a infraestrutura crítica, os países devem ter uma **designação de infraestrutura crítica nacional**, política ou estratégia de cibersegurança com **disposições sobre redução de risco cibernético, medidas de cibersegurança para produtos de TIC que apoiem operações de infraestrutura crítica** e todas as outras medidas incluídas na resolução 58/199 sobre a cultura global de cibersegurança e proteção de infraestruturas de informação crítica (Norma G).
- Além disso, em sua política ou estratégia de cibersegurança, os países devem abordar o **risco da cadeia de abastecimento** e fornecer um **marco apropriado** para preveni-lo e mitigá-lo (Norma I). Relacionado a este ponto pode estar o desenvolvimento e implementação de **normas e marco comuns para a segurança da cadeia de abastecimento** (embora isto esteja além do escopo do que um único país pode alcançar).

	• Outros elementos-chave relevantes para este cenário de ameaça são o desenvolvimento de **regulamentos** que proíbem a introdução de funções ocultas prejudiciais e a exploração de vulnerabilidades em produtos de TIC e o desenvolvimento de **fortes requisitos de segurança da cadeia de abastecimento para os provedores** incorporarem na gestão do ciclo de vida dos produtos de segurança e TIC (Norma I).
Processos e Estruturas	• Particularmente importante para este cenário seria que todos os países envolvidos desenvolvessem e implementassem **mecanismos de governança de risco da cadeia de abastecimento** que envolvessem as principais partes interessadas que representam cada nó da cadeia de valor para coordenar ações e respostas ao ato malicioso (Norma I). • Além disso, para apoiar a comunicação eficaz entre as partes interessadas governamentais e não governamentais, os países devem desenvolver e implementar **processos e procedimentos (incluindo protocolos especialmente para o compartilhamento de evidências digitais) para permitir o compartilhamento de informações** (Norma D). Isto deve incluir processos para aquisição, processamento e armazenamento de dados e informações para investigação e processo penal cibernético. • Em termos de estruturas, é importante estabelecer Pontos de Contato a nível diplomático e técnico (Norma A) para permitir que os governos dos países envolvidos mantenham canais de comunicação abertos e eficientes. • Os países também devem ter **CSIRT/CERT nacionais (ou regionais)** ativos (Normas A, D, G) para mitigar o impacto e minimizar o tempo de recuperação pós-incidente e esses CSIRT/CERT devem ser bem coordenados. • Além da coordenação técnica entre CSIRT/CERT, é importante que os países designem **órgãos nacionais com poderes legais para investigar, processar e fazer cumprir o estado de direito em relação a atos maliciosos no âmbito das TIC**. Essas agências devem ser capazes de interagir e cooperar umas com as outras efetivamente conforme necessário (Normas A, D). • Finalmente, também é essencial um **mecanismo de supervisão** independente e eficaz que garanta a transparência e a responsabilidade pelo funcionamento do Estado (incluindo a coleta de dados) no âmbito das TIC (Normas A, E).

Alianças e Redes	• Em termos de parcerias e redes, há elementos importantes que os países precisam implementar para lidar com as ameaças de manipulação da cadeia de abastecimento. **A cooperação intersetorial entre agências nacionais e o setor privado** (no cenário: a empresa de cibersegurança, o fornecedor de software e outras partes interessadas relevantes) é fundamental para responder adequadamente a ataques à cadeia de abastecimento direcionados, por exemplo, a processos de atualização automática de segurança (Norma A). • Além disso, a **cooperação bilateral, regional e multilateral entre os Estados** com o objetivo de intercambiar informações para efeitos de investigações (inclusive por meio de redes técnicas e policiais) e ação penal (Normas A, D), e para o compartilhamento de conhecimentos sobre medidas destinadas a garantir a integridade da cadeia de abastecimento (Norma I).
Pessoas e Habilidades	• Para responder adequadamente ao cenário, todos os países selecionados necessitariam de especialistas com competências na **gestão de incidentes de cibersegurança** (Norma A), em particular os resultantes de uma cadeia de abastecimento comprometida (Norma I) e com vista a maximizar a eficiência da fase de resposta e recuperação. • Além das habilidades técnicas e de gestão de incidentes, é importante que todos os países envolvidos tenham acesso a **conhecimentos jurídicos** sobre a aplicabilidade do direito internacional no contexto das TIC (Norma A) para assegurar as potenciais implicações jurídicas do incidente, bem como **competências diplomáticas e de comunicação pública** específicas para o contexto de TIC, em particular do país onde o ataque se originou, para gerir de forma eficaz as relações bilaterais com outros países envolvidos e uma comunicação pública mais geral com outros países e partes interessadas (Norma I).
Tecnologia	• Os países e organizações alvo devem estar equipados, ou ter acesso por meio de um parceiro externo, com **capacidade técnica para prevenir, detectar ou interromper ataques à cadeia de abastecimento**. Esses recursos podem incluir, entre outros, plataformas de inteligência de ameaças, sistemas de alerta precoce e, idealmente, ferramentas para avaliação de produtos de TIC.

5. Conclusão

Os três exemplos apresentados no Capítulo 4 ilustram o modo de como medidas específicas concebidas para implementar o Marco para o Comportamento Responsável do Estado no ciberespaço poderiam contribuir para prevenir, ou gerir e reforçar a resposta a uma seleção de atos maliciosos no âmbito das TIC e, por extensão, reforçar resiliência cibernética nacional em geral.

É importante lembrar não apenas que esses são exemplos ilustrativos, mas também elementos importantes de preparação e maturidade cibernética nacional podem não estar diretamente associados ao Marco e, portanto, não foram listados acima. No entanto, o objetivo deste relatório é demonstrar, como complemento, a avaliação mais holística da implementação nacional do Marco apresentada na Parte I deste estudo[12] — como uma abordagem mais focada com base em perfis de ameaças específicos pode adicionar uma camada adicional de análise que pode melhorar ainda mais a compreensão de um Estado sobre suas atuais capacidades cibernéticas.

No preâmbulo do Capítulo 4, é mencionado como, independentemente do perfil da ameaça, determinadas normas e capacidades fundamentais associadas devem ser consideradas relevantes

12 Consulte Samuele Dominioni e Giacomo Persi Paoli. 2023. Descobrindo as necessidades de desenvolvimento de habilidades cibernéticas: Parte I. Classificando as habilidades cibernéticas fundamentais. JUNTAR.

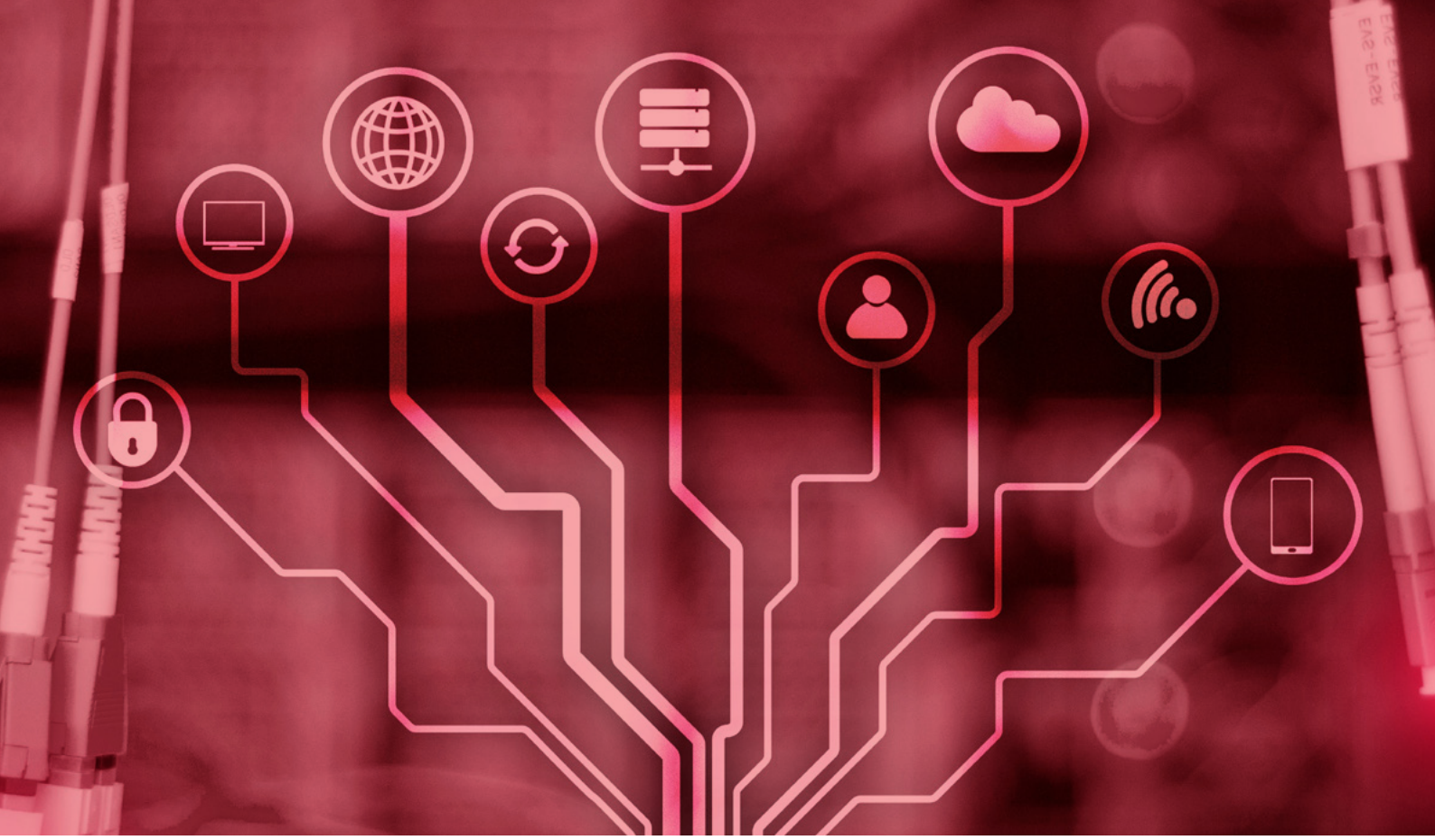
e aplicáveis independentemente do cenário ou ameaça em questão. Trata-se da Norma A relativa à cooperação entre Estados e a Norma E sobre direitos humanos. A análise dos três cenários baseia-se neste ponto e identifica outras FCC específicas que parecem ser recorrentes em várias ameaças e em várias normas.

Do ponto de vista político e regulamentar, os Estados devem dar prioridade ao desenvolvimento (e a revisão periódica) de estratégias e políticas nacionais abrangentes de cibersegurança que, em combinação com as leis apropriadas, permitam aos Estados tomar todas as medidas necessárias a nível nacional e internacional para garantir a proteção do âmbito das TIC, inclusive através da cooperação entre as várias partes interessadas. Além disso, os Estados devem dar prioridade ao desenvolvimento de posições públicas e abrangentes sobre como o direito internacional se aplica ao âmbito das TIC.

Do ponto de vista do processo, os Estados devem dar prioridade ao desenvolvimento de mecanismos que facilitem a cooperação em matéria de segurança das TIC com todas as partes interessadas nacionais relevantes, incluindo agências governamentais, setor privado e a comunidade técnica, bem como a sociedade civil, conforme apropriado. Isto garantiria não só fluxos de informação oportunos, eficientes e eficazes em tempos de crise, mas também o acesso a ativos de conhecimento que podem ser aproveitados conforme apropriado para compensar a potencial escassez de expertise disponível no setor público. Da mesma forma, os Estados devem desenvolver mecanismos para facilitar a cooperação e o compartilhamento de informações nos níveis bilateral, regional e internacional. O desenvolvimento de processos e mecanismos específicos permitiria a criação de **parcerias e redes que funcionem**.

Em relação às estruturas, os Estados deveriam dar prioridade ao desenvolvimento e a sustentabilidade de capacidades nacionais totalmente operacionais de resposta a incidentes informáticos que são elementos insubstituíveis da primeira linha de defesa contra atos maliciosos contra as TIC. Vários acordos nacionais e regionais entre CSIRT/CERT públicos e privados poderiam ser explorados para atender as limitações de recursos, habilidades ou tecnologias. Além disso, os Estados deveriam dar prioridade à identificação de agências responsáveis dentro do governo nacional para atuar como pontos focais para questões das TIC nos níveis político e técnico, inclusive com a criação de um Ponto de Contato Nacional dedicado. A presença de uma unidade com autoridade e poderes para investigar e processar atos maliciosos relacionados com as TIC parece ser um requisito transversal. Embora todos os setores sofram de escassez de habilidades cibernéticas, a implementação bem-sucedida do Marco dependerá da capacidade dos Estados de desenvolver internamente, ou acederem através de parcerias externas, **conhecimentos técnicos e jurídicos adequados** para poder gerir eficazmente incidentes das TIC a nível nacional e garantir o cumprimento como o Marco, mas também para se comprometer de forma construtiva com os seus homólogos a nível internacional em questões relacionadas com a segurança das TIC. Isto também se tornará uma demanda crescente de diplomatas, que devem reforçar sua compreensão das questões relacionadas com as TIC e ser apoiados por especialistas e consultores quando necessário.

Finalmente, a implementação bem-sucedida do Marco também dependerá da capacidade de um Estado de acessar um certo número de **tecnologias e soluções técnicas**, quer desenvolvendo-as em nível nacional, quer acedendo a elas através de parcerias com outros (por exemplo, acordos bilaterais ou regionais com outros Estados, ou parcerias público-privadas). Estas soluções tecnológicas incluem, mas não se limitam a, capacidades para prevenir, detectar e interromper diferentes tipos de ataques (por exemplo, plataformas de inteligência de ameaças, sistemas de alerta precoce) e soluções para aumentar a confidencialidade, integridade e disponibilidade de sistemas e dados (por exemplo, centros de dados baseados na nuvem).



Anexo 1. Tabela de Capacidades Cibernéticas Fundamentais

Norma A

Os Estados devem cooperar no desenvolvimento e aplicação de medidas para aumentar a estabilidade e segurança no uso das TIC e prevenir práticas de TIC reconhecidas como nocivas ou que possam representar uma ameaça à paz e segurança internacionais.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Política e estratégia de cibersegurança (e plano de implementação nacional) ou legislação nacional de cibersegurança (de preferência com uma abordagem de todo o governo).
iii	Abordagem de gestão de riscos cibernéticos (incluindo infraestruturas críticas).
iv	Política externa que reconhece a cibersegurança como uma das prioridades.
v	Compromisso público com o Marco de Comportamento Responsável dos Estados no ciberespaço.
vi	Declaração pública sobre capacidades cibernéticas nacionais disponível (informação não classificada).
vii	Estratégias e planos nacionais para o desenvolvimento de competências cibernéticas.
ESTRUTURAS E PROCESSOS	
i	Centro nacional, agência ou entidade responsável pela cibersegurança.
ii	Capacidades nacionais ou regionais de detecção e resposta a incidentes cibernéticos (por exemplo, CERT/CSIRT ou um Centro de Operações de Segurança).
iii	Ponto de contato (PoC) a nível diplomático e técnico.
iv	Cooperação e compartilhamento de informações entre a legislação e a aplicação da lei.
v	Mecanismos de supervisão independentes e eficazes (judicial, administrativo, parlamentar) capazes de garantir a transparência e a responsabilização relativamente ao funcionamento do Estado no âmbito das TIC.
ASSOCIAÇÕES E REDES	
i	Cooperação intrasetorial (setor privado, sociedade civil, comunidade técnica, academia).
ii	Cooperação intragovernamental (por exemplo, reuniões interministeriais, grupos de trabalho).
iii	Cooperação bilateral, regional e multilateral em diferentes níveis (técnico, operacional, diplomático).
iv	Acordos multilaterais (por exemplo, a Convenção de Budapeste, a Convenção de Malabo).
PESSOAS E HABILIDADES	
i	Capacidades diplomáticas para participar em processos internacionais e intergovernamentais.
ii	Especialistas e profissionais de políticas com conhecimento básico de cibersegurança.
iii	Juristas com competências jurídicas em direito internacional relacionadas com atividades no âmbito das TIC.
iv	Programas de “formação de formadores” e certificação profissional.
v	Competências para gerir incidentes de cibersegurança, incluindo preparação, resposta e recuperação, tanto a nível nacional como internacional.
vi	Campanhas sistemáticas de sensibilização, dirigidas ao público em geral, sobre a importância dos patches de segurança e outras práticas básicas de ciber-higiene como as atualizações de software.
TECNOLOGIA	
i	Capacidades para garantir a cibersegurança nos pontos terminais (antivírus ou atualizações automáticas e patches de produtos digitais para mitigar erros e vulnerabilidades de segurança).
ii	Capacidades técnicas para prevenir, detectar ou interromper atos maliciosos relacionados com as TIC.
iii	Soluções técnicas para proteger as comunicações (por exemplo, criptografia).

Norma B

No caso de incidentes de TIC, os Estados devem considerar todas as informações relevantes, incluindo o contexto mais amplo do evento, as dificuldades de atribuição no ambiente de TIC e a natureza e extensão das consequências.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Posição(ões) ou declaração(ões) nacional(is) sobre a aplicação do direito internacional ao uso das TIC pelos Estados.
iii	Classificação (pública ou não pública) de incidentes de TIC em termos de escala e impacto.
iv	Política de atribuição (pública ou não pública) que inclui definições, metodologia e funções e responsabilidades claras.
v	Regulamento que permite a compartilhamento de informações com entidades comerciais relevantes e outras entidades não governamentais.
ESTRUTURAS E PROCESSOS	
i	Critérios de evidência nacional para determinar a atribuição.
ii	Processos e procedimentos que permitem o compartilhamento de informações entre as entidades governamentais e não governamentais relevantes.
ASSOCIAÇÕES E REDES	
i	Cooperação entre as partes interessadas nacionais (por exemplo, grupos de trabalho, plataformas de múltiplas partes interessadas.
ii	Cooperação bilateral e multilateral em questões de assistência internacional e compartilhamento de informações.
iii	Cooperação bilateral e multilateral para a solução de divergências e controvérsias por meio de consultas e outros meios pacíficos.
PESSOAS E HABILIDADES	
i	Habilidades para realizar (ou avaliar, se a informação for fornecida por terceiros) investigações técnicas de incidentes de TIC.
ii	Funcionários públicos (incluindo pessoal diplomático) com competências jurídicas específicas no contexto das TIC, incluindo consultas e outros meios pacíficos para resolver disputas à escala internacional.
iii	Funcionários públicos (incluindo funcionários diplomáticos) com habilidades de negociação e comunicação específicas para o contexto de TIC.
TECNOLOGIA	
i	Capacidades técnicas e forenses para investigar e determinar a origem da atividade maliciosa relacionada às TIC.

Norma C

Os Estados não devem permitir conscientemente que seu território seja usado para cometer atos internacionalmente ilícitos usando as TIC.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma, incluindo a opinião do Estado sobre o que constitui ato internacionalmente ilícito de uso das TIC.
ii	Estratégia e política de cibersegurança, incluindo disposições para prevenir, detectar e interromper o uso malicioso de TIC.
iii	Legislação específica que define quais tipos de atividades de TIC são e não são permitidas no território e que outorga autoridade para investigar, encerrar ou processar esses tipos de atividades.
ESTRUTURAS E PROCESSOS	
i	Capacidades nacionais ou regionais de detecção e resposta a incidentes cibernéticos (por exemplo, CERT/CSIRT ou um Centro de Operações de Segurança).
ii	Capacidade de aplicação da lei cibernética.
iii	Procedimento para compartilhamento de informações entre as partes interessadas nacionais relevantes, incluindo entidades não governamentais.
iv	Mecanismos para enviar ou responder a solicitações de assistência (incluindo procedimentos para avaliar solicitações).
ASSOCIAÇÕES E REDES	
i	Cooperação entre as partes interessadas nacionais (por exemplo, grupos de trabalho, plataformas de múltiplas partes interessadas), incluindo parcerias público-privadas relevantes.
ii	Acordos bilaterais e multilaterais sobre questões de assistência e compartilhamento de informações.
iii	Marco para compartilhamento de informações em nível técnico (como a rede FIRST).
PESSOAS E HABILIDADES	
i	Capacidade de identificar e interromper atos maliciosos que usam TIC alocados em seu próprio território.
ii	Funcionários públicos (incluindo pessoal diplomático) com competências de comunicação específicas para o contexto das TIC.
TECNOLOGIA	
i	Capacidade técnica para prevenir, detectar ou interromper atos maliciosos relacionados com as TIC alocados no seu próprio território.

Norma D

Os Estados devem considerar a melhor forma de cooperar para o compartilhamento de informações, prestarem assistência mútua, processar o uso terrorista e criminoso das TIC e implementar outras medidas de cooperação para enfrentar esse tipo de ameaça.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Assinatura e ratificação de instrumentos bilaterais, regionais ou multilaterais sobre crimes cibernéticos.
iii	Políticas que descrevam os mecanismos ou procedimentos de cooperação e compartilhamento de informações, que devem incluir entidades comerciais e outras entidades não governamentais relevantes.
iv	Legislação sobre crimes cibernéticos que garante uma abordagem tecnologicamente neutra.
ESTRUTURAS E PROCESSOS	
i	Mecanismo de envio ou resposta a pedidos de assistência (por exemplo, pedidos de assistência jurídica mútua).
ii	Protocolos e procedimentos para coletar, tratar e armazenar evidências digitais.
iii	Capacidade de aplicação da lei cibernética.
iv	Recursos nacionais ou regionais de detecção e resposta a incidentes cibernéticos (por exemplo, CERT/CSIRT ou um Centro de Operações de Segurança).
ASSOCIAÇÕES E REDES	
i	Cooperação bilateral, regional e multilateral para investigação, assistência, aplicação da lei e compartilhamento de informações sobre o uso criminoso e terrorista das TIC (por exemplo, tratados de assistência jurídica mútua).
ii	Redes operacionais (por exemplo, INTERPOL I-24/7) e técnicas (por exemplo, FIRST).
iii	Cooperação entre as partes interessadas nacionais relevantes (por exemplo, grupos de trabalho, plataformas multissetoriais), inclusive por meio de parcerias público-privadas estruturadas.
PESSOAS E HABILIDADES	
i	Capacidade de lidar com evidências digitais a nível técnico e legal.
ii	Conhecimento da legislação sobre cibercrime e terrorismo em outros Estados-membros.
iii	Capacidade de construir relacionamentos com contrapartes e parceiros bilaterais, regionais e internacionais para garantir que as intervenções sejam eficientes e oportunas.
TECNOLOGIA	
i	Capacidade técnica para prevenir, detectar ou interromper atos maliciosos relacionados às TIC por criminosos e terroristas.
ii	Canais de comunicação ou plataformas seguras para compartilhar informações.

Norma E

Os Estados, ao garantir o uso seguro das TIC, devem garantir o pleno respeito aos direitos humanos, incluindo o direito à liberdade de expressão.

POLÍTICAS E REGULAMENTOS	
i	Posição nacional sobre como o direito internacional é aplicado, incluindo o direito internacional dos direitos humanos.
ii	Políticas e estratégias de cibersegurança consistentes com a lei internacional de direitos humanos (por exemplo, orientação nas resoluções 68/167 e 69/166).
iii	Não imponha restrições indevidas à liberdade de expressão e à liberdade de procurar, receber e transmitir informações.
iv	Regulamentos, inclusive para empresas, relativas ao respeito aos direitos humanos na concepção, desenvolvimento e uso de novas tecnologias.
v	Legislação sobre vigilância e interceptação pelo Estado, de acordo com o direito à privacidade.
vi	Leis de proteção de dados.
ESTRUTURAS E PROCESSOS	
i	Mecanismos de fiscalização nacionais ou regionais independentes e eficazes (judicial, administrativo ou parlamentar) capazes de garantir a transparência e a responsabilização relativamente à vigilância das comunicações, interceptação e coleta de dados pessoais pelo Estado.
ASSOCIAÇÕES E REDES	
i	Participar e consultar as partes interessadas que defendem, promovem e analisam os direitos humanos e as liberdades fundamentais online para entender e minimizar os possíveis impactos negativos das políticas sobre os indivíduos.
PESSOAS E HABILIDADES	
i	Funcionários públicos (incluindo aqueles que trabalham na aplicação da lei) com conhecimento de direitos humanos no âmbito digital, bem como de como implementar instrumentos internacionais de maneira consistente com os direitos humanos.
ii	Conhecimentos especializados sobre direitos humanos e contextualizados, inclusive na área jurídica.
TECNOLOGIA	
i	Capacidade tecnológica para garantir o respeito aos direitos humanos no uso das TIC por atores estatais e não estatais.

Norma F

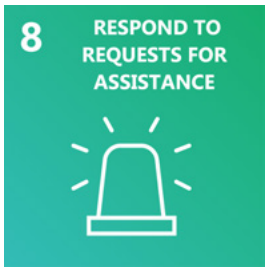
Um Estado não deve conduzir ou apoiar conscientemente uma atividade de TIC contrária às suas obrigações ao abrigo do direito internacional que intencionalmente danifique ou prejudique a infraestrutura crítica.

POLÍTICAS E REGULAMENTOS	
i	Posição nacional sobre a aplicabilidade do direito internacional no uso das TIC pelos Estados.
ii	Interpretação nacional da norma.
iii	Classificação (pública ou não pública) de incidentes de TIC em termos de escala e gravidade.
iv	Concepção nacional de infraestrutura crítica.
ESTRUTURAS E PROCESSOS	
i	Mecanismos de supervisão nacionais ou regionais independentes e eficazes (judicial, administrativo, parlamentar) capazes de garantir a transparência, conforme o caso.
ASSOCIAÇÕES E REDES	
i	Marcos de cooperação bilateral, regional e multilateral para cooperação e compartilhamento de informações.
PESSOAS E HABILIDADES	
i	Conhecimento especializado do direito internacional aplicável especificamente às atividades desenvolvidas no âmbito das TIC.
TECNOLOGIA	
N/D	

Norma G

Os Estados devem tomar medidas apropriadas para proteger sua infraestrutura crítica contra ameaças relacionadas às TIC.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Designação nacional de setores de infraestrutura críticos.
iii	Classificação (pública ou não pública) de incidentes de TIC em termos de escala e gravidade.
iv	Legislação para proteção de infraestrutura crítica (estabelecimento de normas, relatórios, auditorias etc.).
v	Estratégia e política de cibersegurança que inclui disposições sobre redução de risco cibernético em infraestrutura crítica e medidas de cibersegurança para produtos de TIC, e que leva em consideração a resolução 58/199 sobre a cultura global de cibersegurança e proteção de infraestrutura crítica de informação.
vi	Regulamento que permite a compartilhamento de informações com entidades comerciais relevantes e outras entidades não governamentais.
ESTRUTURAS E PROCESSOS	
i	Centro(s) ou agência(s) nacional(is) responsável(is) pela infraestrutura crítica.
ii	ii. Capacidades nacionais ou regionais de detecção e resposta a incidentes cibernéticos (por exemplo, CERT/CSIRT ou um Centro de Operações de Segurança).
iii	Mecanismos de cumprimento das medidas de cibersegurança na infraestrutura crítica.
iv	Planos de contingência em caso de incidentes de TIC que envolvam infraestrutura crítica.
v	Processos e procedimentos que permitem o compartilhamento de informações entre as entidades governamentais e não governamentais relevantes.
ASSOCIAÇÕES E REDES	
i	Cooperação transfronteiriça com operadores e proprietários de infraestrutura relevante (por exemplo, coordenação de respostas a incidentes, compartilhamento de boas práticas de proteção de dados, infraestrutura crítica).
ii	Cooperação entre partes interessadas nacionais relevantes (por exemplo, comitês interinstitucionais, plataformas multissetoriais), incluindo parcerias público-privadas e proprietários, operadores ou administradores de propriedade de infraestrutura crítica.
PESSOAS E HABILIDADES	
i	Habilidades técnicas para proteger a infraestrutura crítica nacional contra atos maliciosos envolvendo TIC.
ii	Treinamentos e exercícios que visam melhorar a capacidade de resposta e testar a continuidade dos serviços e planos de contingência para ataques a infraestruturas críticas e que estimulem os interessados a participar de atividades similares.
iii	Pessoal diplomático com capacidade para **interagir significativamente com seus homólogos sobre o tema específico das infraestruturas críticas**, especialmente se estas forem transnacionais.
TECNOLOGIA	
i	Capacidade técnica para prevenir, detectar ou interromper atos maliciosos contra infraestruturas críticas relacionadas com as TIC.



Norma H

Os Estados devem responder às solicitações apropriadas de assistência de outro Estado cuja infraestrutura crítica esteja sujeita a atos maliciosos de TIC.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Legislação que fornece um marco para solicitar e fornecer assistência internacional.
iii	Estratégias e políticas de cibersegurança que descrevem os mecanismos, procedimentos e processos para responder a solicitações de assistência.
ESTRUTURAS E PROCESSOS	
i	Mecanismos eficientes para receber, processar, avaliar e responder aos pedidos de assistência, bem como para os preparar e enviar.
ii	Capacidade de aplicação da lei cibernética.
ASSOCIAÇÕES E REDES	
i	Cooperação bilateral, regional e multilateral para a proteção de infraestrutura crítica (por exemplo, criação de modelos comuns para solicitação de assistência, assinatura de Memorandos de Entendimento etc.).
ii	Cooperação transfronteiriça com os principais proprietários e operadores de infraestrutura, bem como provedores (por exemplo, co-ordenação de sistemas de alerta de emergência e compartilhamento e análise de informações de vulnerabilidade).
iii	Cooperação entre as partes interessadas relevantes (por exemplo, parcerias público-privadas e comissões interinstitucionais).
PESSOAS E HABILIDADES	
i	Capacidade de fornecer assistência transfronteiriça eficaz e oportuna aos Estados que estão sob ataque contra infraestrutura crítica.
ii	Habilidades para atender e gerir pedidos de assistência.
TECNOLOGIA	
i	Capacidade técnica para prevenir, detectar ou interromper atos maliciosos contra infraestruturas críticas relacionadas com as TIC.
ii	Canais de comunicação ou plataformas seguras para compartilhamento de informações relacionadas a atos maliciosos contra in-fraestruturas críticas que envolvam TIC.

Norma I

Os Estados devem tomar medidas razoáveis para garantir a integridade da cadeia de abastecimento e tentar impedir a proliferação de ferramentas e técnicas de TIC maliciosas e o uso de funções nocivas ocultas.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Leis e regulamentos que proíbem a introdução de funções ocultas prejudiciais e a exploração de vulnerabilidades em produtos de TIC.
iii	Política e estratégia de cibersegurança que abranja a segurança da cadeia de abastecimento e descreva marcos importantes.
iv	Obrigação de implementar regras e normas comuns globalmente interoperáveis para segurança da cadeia de abastecimentos (por exemplo, ISO/IEC 20243).
v	Exigir que os provedores incorporem segurança e proteção no gerenciamento do ciclo de vida de seus produtos de TIC.
ESTRUTURAS E PROCESSOS	
i	Mecanismo de governança para gestão de riscos na cadeia de abastecimento, que deve incluir os atores-chave que representam os nós da cadeia de valor.
ii	Mecanismo de avaliação e certificação de produtos TIC (nacionais ou em aliança com outros países).
iii	Acordos para garantir a interoperabilidade de abordagens, métodos de certificação e certificações de produtos de TIC entre jurisdições.
ASSOCIAÇÕES E REDES	
i	Medidas de cooperação a nível bilateral, regional e multilateral para, por exemplo, o compartilhamento de boas práticas de gestão de riscos na cadeia de abastecimento ou a certificação de produtos TIC.
PESSOAS E HABILIDADES	
i	Capacidades em questões de segurança e gestão de riscos da cadeia de abastecimento.
ii	Habilidades de resposta e gerenciamento de incidentes.
iii	Pessoal diplomático com capacidade para **interagir significativamente com seus homólogos sobre o tema específico das infraestruturas críticas**, especialmente se estas forem transnacionais.
TECNOLOGIA	
i	Capacidade técnica para prevenir, detectar ou interromper ataques às cadeias de abastecimento.

Norma J

Os Estados devem encorajar a notificação responsável de vulnerabilidades de TIC e compartilhar as informações correspondentes sobre soluções disponíveis para essas vulnerabilidades, a fim de limitar e possivelmente eliminar ameaças potenciais às TIC e à infraestrutura dependente de TIC.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Medidas legais para impedir a distribuição comercial de vulnerabilidades.
iii	Descriminalização e proteção legal para pesquisadores de segurança e *hackers* éticos que desejam expor vulnerabilidades.
iv	Política de divulgação de vulnerabilidade coordenada (CVD).
v	Marcos jurídicos que permitem a cooperação e o compartilhamento de informações com vendedores e provedores.
vi	vRequisitos que uma política e prática de gestão de vulnerabilidade eficiente e eficaz devem atender.
ESTRUTURAS E PROCESSOS	
i	Orientação sobre as respectivas funções e responsabilidades das diferentes partes interessadas nos processos de notificação de vulnerabilidade, incluindo os tipos de informações técnicas a serem divulgadas e tratamento de dados confidenciais etc.
ii	Protocolos estabelecidos para comunicação e compartilhamento de informações entre todas as partes interessadas relevantes (por exemplo, governos, vendedores e provedores, pesquisadores de segurança, equipes de resposta a incidentes). Protocolos estabelecidos para atualização e patching de sistemas, particularmente aqueles relacionados a infraestruturas dependentes de TIC.
iii	Orientação e incentivos para divulgação coordenada de vulnerabilidades (por exemplo, programas de recompensas por detecção de erros).
iv	Campanhas sistemáticas de conscientização (dirigidas tanto ao público em geral quanto a profissionais de setores específicos, principalmente aqueles que atuam em setores de infraestrutura crítica) sobre a importância dos patches de segurança.
ASSOCIAÇÕES E REDES	
i	Cooperação bilateral, regional e multilateral para a divulgação de vulnerabilidades.
ii	Cooperação intersetorial com o setor privado, sociedade civil e comunidade técnica, incluindo provedores e proprietários.
PESSOAS E HABILIDADES	
i	Habilidades técnicas para identificar e resolver vulnerabilidades ou gerenciar informações relacionadas a vulnerabilidades recebidas de terceiros (por exemplo, empresas que oferecem recompensas por detecção de erros, pesquisadores de segurança, provedores).
ii	Habilidades de comunicação pública necessárias para lidar com vulnerabilidades, especialmente quando elas têm impacto na população em geral.
iii	Habilidades diplomáticas e de comunicação necessárias para poder participar com sucesso em discussões de gerenciamento de vulnerabilidade com atores estatais e não estatais relevantes.
TECNOLOGIA	
i	Capacidade técnica para identificar e resolver vulnerabilidades de TIC ou para agir quando a informação é fornecida por terceiros.
ii	Capacidade técnica para instalar patches de grande escala.

Norma K

Os Estados não devem conduzir ou apoiar intencionalmente atividades que danifiquem os sistemas de informação das equipes autorizadas de resposta a emergências (às vezes conhecidas como equipes de resposta a emergências informáticas ou equipes de resposta a incidentes de cibersegurança) de outro Estado. Um Estado não deve usar equipes de resposta a emergências autorizadas para se envolver em atividades internacionais maliciosas.

POLÍTICAS E REGULAMENTOS	
i	Posição nacional sobre a norma (ou certos aspectos dela).
ii	Declaração pública de que o Estado não utilizará equipes autorizadas de resposta a emergências para participar de atividades internacionais maliciosas ou ofensivas e que respeitará os princípios éticos que norteiam o trabalho dessas organizações.
iii	Lista de todos os CERT/CSIRT declarados.
iv	Política ou estratégia de cibersegurança que descreve claramente o status (por exemplo, infraestrutura crítica), autoridade e mandatos de CERTs/CSIRTs, juntamente com o que distingue suas funções únicas e neutras de outras funções governamentais.
v	Marco regulamentar para o trabalho dos CERTs/CSIRTs alinhado com as diretrizes e normas internacionais (por exemplo, o código de ética FIRST ou ISO 27/2001).
ESTRUTURAS E PROCESSOS	
i	Capacidades nacionais ou regionais de resposta a incidentes cibernéticos (por exemplo, CERTs/CSIRTs ou um Centro de Operações de Segurança).
ii	Mecanismos de supervisão independentes e eficazes (judicial, administrativo, parlamentar) capazes de garantir a transparência e a responsabilização relativamente ao funcionamento do Estado no domínio das TIC.
ASSOCIAÇÕES E REDES	
N/D	
PESSOAS E HABILIDADES	
i	Habilidades para conduzir (ou avaliar, se as informações forem fornecidas por terceiros) investigações técnicas sobre o uso indevido do CERT ou CSIRT para conduzir atividades maliciosas.
ii	Funcionários públicos (incluindo militares) cientes do papel e status dos CERT/CSIRT.
iii	Conhecimento especializado sobre direito internacional aplicável especificamente no âmbito das TIC.
TECNOLOGIA	
N/D	

Direito Internacional

Observação: esta seção da tabela da FCC inclui elementos adicionais da lei internacional que devem ser considerados complementares ou suplementares àqueles especificamente incluídos em cada regra.

POLÍTICAS E REGULAMENTOS	
i	Declaração pública de como o Estado entende a aplicação do direito internacional ao ciberespaço.
ESTRUTURAS E PROCESSOS	
i	Mecanismos de fiscalização independentes (judicial, administrativo, parlamentar) capazes de garantir a legalidade e a responsabilização relativamente às operações do Estado no âmbito das TIC.
ASSOCIAÇÕES E REDES	
i	Cooperação com outros Estado-membros nas áreas de direito internacional, legislação e políticas nacionais.
ii	Participação em processos multilaterais relacionados com o direito internacional na área das TIC.
PESSOAS E HABILIDADES	
i	Conhecimento especializado em direito internacional eas responsabilidades dos Estados no âmbito cibernético.
ii	Capacidade de participar de discussões regionais e internacionais sobre direito internacional, incluindo a capacidade de interagir com a comunidade acadêmica e a sociedade civil em geral, em um idioma que pode não ser a língua materna.
TECNOLOGIA	
N/D	

Medidas de Construção de Confiança

POLÍTICAS E REGULAMENTOS	
i	Divulgação pública de todas as estratégias, políticas e regulamentos nacionais de cibersegurança relevantes, de preferência com uma tradução oficial para o inglês (no mínimo) para facilitar o acesso e a transparência.
ii	Identificar e considerar MFC apropriados em seus contextos específicos e cooperar com outros Estados em sua implementação.
ESTRUTURAS E PROCESSOS	
i	Estabelecimento de Pontos de Contacto (PoC) nacionais ao nível diplomático e técnico.
ii	Capacidades nacionais ou regionais de resposta a incidentes cibernéticos (por exemplo, CERT/CSIRT ou um Centro de Operações de Segurança).
iii	Compartilhar informações e boas práticas, lições ou livros brancos sobre: • ameaças e incidentes existentes e emergentes relacionados à segurança de TIC; • estratégias e normas nacionais para a análise de vulnerabilidades em produtos de TIC; • abordagens nacionais e regionais para gestão de riscos e prevenção de conflitos.
iv	Compartilhamento de informações sobre: • abordagens nacionais para segurança de TIC; • proteção de dados; • proteção de infraestrutura crítica dependente de TIC; • a missão e funções do órgão responsável pela segurança das TIC, a estratégia de TIC a nível nacional ou organizacional e os regimes legais e de supervisão em que operam.
ASSOCIAÇÕES E REDES	
i	Participação em processos das Nações Unidas (por exemplo, OEWG).
ii	Participar do diálogo por meio de consultas bilaterais, sub-regionais, regionais e multilaterais.
iii	Participar em/com órgãos regionais que desenvolvem e implementam as MFCs.
iv	Participar de estruturas de cooperação entre CERT/CSIRT ou outros órgãos técnicos de segurança, como a rede FIRST ou outros marcos regionais.
PESSOAS E HABILIDADES	
i	Conhecimento das MFCs existentes e formas de ativá-los ou aproveitá-los em tempos de crise.
ii	Conhecimento e competências necessários para atuar efetivamente como PoC nacional (se nomeado).
iii	Capacidade de fazer uso de plataformas de compartilhamento de informações existentes (por exemplo, portal de políticas cibernéticas UNIDIR).
iv	Habilidades diplomáticas e de comunicação necessárias para participar efetivamente em debates sobre cibersegurança com seus homólogos em outros países.
TECNOLOGIA	
i	Canais e plataformas confiáveis de comunicação entre os Estados.

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG