CADERNOS CGI.br Referências

7

Promovendo a Ciberestabilidade

Comissão Global sobre a Estabilidade do Ciberespaço

cgi.br
Comitê Gestor da Internet no Brasil

Núcleo de Informação
e Coordenação do Ponto BR

07

CADERNOS CGI.br **Referências**

Promovendo a Ciberestabilidade

Comissão Global sobre a Estabilidade do Ciberespaço

Relatório Final - Novembro de 2019

Comitê Gestor da Internet no Brasil
Outubro 2022

Núcleo de Informação e Coordenação do Ponto BR

Diretor Presidente
Demi Getschko

Diretor de Assessoria às Atividades do CGI.br
Hartmut Richard Glaser

Diretor Administrativo
Ricardo Narchi

Diretor de Serviços e Tecnologia
Frederico Neves

Diretor de Projetos Especiais e de Desenvolvimento
Milton Kaoru Kashiwakura

Produção dos Cadernos CGI.br
Diretoria de Assessoria às Atividades do CGI.br

Coordenação Executiva e Editorial
Carlos Francisco Cecconi e Jean Carlos Ferreira dos Santos

Produção Editorial
Carolina Carvalho (Comunicação NIC.br)

Produção desta publicação

Tradução
Ana Zuleika Pinheiro Machado

Projeto Gráfico e Ilustrações
Pilar Velloso

Revisão da Tradução
Bruna Toso de Alcântara e Vinicius Wagner Oliveira Santos

Revisão Técnica e Preparação
Bruna Toso de Alcântara, Carlos Francisco Cecconi, Jean Carlos Ferreira dos Santos e Vinicius Wagner Oliveira Santos

Diagramação
Daniele Doneda

Fotos
Shutterstock

Título original
Advancing cyberstability: final report November 2019.
Disponível em: <https://cyberstability.org/report>

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Promovendo a ciberestabilidade [livro eletrônico] / Comissão Global sobre a Estabilidade do Ciberespaço; tradução Ana Zuleika Pinheiro Machado. -- São Paulo, SP; Comitê Gestor da Internet do Brasil, 2022. PDF
Título original: Advancing cyberstability: final report november 2019.
ISBN 978-65-86949-71-1
1. Ciberespaço
2. Internet - Leis e legislação
3. Segurança cibernética I. Comissão Global sobre a Estabilidade do Ciberespaço. II. Título.
22-118779 CDD-006.6

Índices para catálogo sistemático:
1. Ciberespaço: Ciência da computação 006.6
Eliete Marques da Silva - bibliotecária - CRB-8/9380

Esta publicação está disponível também em formato digital em <http://www.cgi.br>

Comitê Gestor da Internet no Brasil (CGI.br)

Composição em Outubro de 2022

Integrantes

Representantes do Setor Governamental
Carlos Manuel Baigorri
Cláudio Furtado
Evaldo Ferreira Vilela
Fernando André Coelho Mitkiewicz
Jackline de Souza Conca
Jeferson Denis Cruz de Medeiros
José Gustavo Sampaio Gontijo
Maximiliano Salvadori Martinhão
Orlando Oliveira dos Santos

Representantes do Setor Empresarial
Henrique Faulhaber
José Alexandre Novaes Bicalho
Nivaldo Cleto
Rosauro Leandro Baretta

Representantes do Terceiro Setor
Bia Barbosa
Domingos Sávio Mota
Laura Conde Tresca
Percival Henriques de Souza Neto

Representantes da Comunidade Científica e Tecnológica
Marcos Dantas Loureiro
Rafael de Almeida Evangelista
Tanara Lauschner

Representante de notório saber em assuntos de Internet
Demi Getschko

Coordenador
José Gustavo Sampaio Gontijo

Secretário Executivo
Hartmut Richard Glaser

Apresentação

por MARÍLIA MACIEL

Um mundo em que atores públicos e privados atuem em comum, galvanizados ao redor de um núcleo duro de normas, cujo objetivo é promover a estabilidade, a paz e a prosperidade no ciberespaço. Essa foi a visão que inspirou três anos de trabalho da Comissão Global sobre a Estabilidade do Ciberespaço, capturados no presente relatório.

A clareza em relação ao objetivo final proporcionou as balizas necessárias para agregar um grupo extremamente diverso de membros. Vinte e oito Comissários provenientes da comunidade técnica, academia, setor privado, sociedade civil, e setor público uniram esforços para pensar sobre a governança da segurança cibernética.

Os vários elementos constitutivos da noção de 'governança' foram objeto de discussão no âmbito da Comissão. Princípios de base foram identificados, normas foram definidas, processos de discussão e consulta foram delineados, e uma ampla gama de atores foram apontados como essenciais para a promoção da estabilidade. Dentre esses elementos, a Comissão decidiu dar ênfase à elaboração de normas, fazendo deste o principal produto do seu trabalho.

Nos últimos anos é possível perceber uma intensa atividade normativa no âmbito da segurança cibernética. Normas representam crenças compartilhadas no seio de uma comunidade[1], e são importantes instrumentos de alinhamento de condutas, uma vez que descrevem as expectativas coletivas para o comportamento adequado dos atores[2].

Normas são particularmente necessárias em um contexto no qual se multiplicam os fatores entrópicos e desestabilizadores

1 Finnemore, M. Cybersecurity and the Concept of Norms. Carnegie Endowment for International Peace, 2017. Disponível em: <https://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870>

2 Katzenstein, P. Introduction: Alternative Perspectives on National Security In Katzenstein, P (ed.) The Culture of National Security: Norms and Identity in World Politics. New York: Columbia University Press, 1996.

no âmbito do ciberespaço. Por um lado, um número crescente de países têm investido em capacidades cibernéticas ofensivas, contribuindo para diluir as linhas que separam as operações tradicionais das cibernéticas. Por outro lado, a facilidade de acesso aos meios para perpetrar um ataque ampliou o grupo de atores capazes de se engajar em condutas maliciosas com motivações econômicas, políticas ou criminosas.

A pandemia de Covid-19 agravou o panorama de ameaças à estabilidade, pois levou a uma acelerada digitalização, multiplicando os pontos de vulnerabilidade[3]. Vários setores, como finanças, saúde, e energia, estão se tornando digitalizados. Instituições públicas também estão desenvolvendo seus próprios serviços eletrônicos, muitos dos quais se mostraram essenciais em tempos de crise.

Em 2015, a Assembleia Geral da ONU endossou 11 normas voluntárias visando a estimular o comportamento responsável dos Estados no ciberespaço, contidas no relatório do Grupo de Especialistas Governamentais da ONU de 2013-2015 (GGE 2015). Paralelamente, iniciativas não-governamentais focadas na elaboração de normas e princípios - como é o caso da Comissão Global sobre a Estabilidade do Ciberespaço - também floresceram nos últimos anos. Este é um desenvolvimento importante porque os processos da ONU permanecem intergovernamentais e as normas neles desenvolvidas são direcionadas aos Estados, mesmo que afetem indiretamente outros atores.

Iniciativas não-governamentais para a elaboração de normas ampliam o grupo de agentes engajados na promoção da estabilidade cibernética, atribuindo papéis e responsabilidades às empresas, à comunidade técnica e aos indivíduos. Essa responsabilização é fundamental em um cenário em que governos inescapavelmente dependem da colaboração de outros setores para a co-criação de um regime eficaz e sustentável de governança da segurança cibernética.

Mesmo diante de uma atividade normativa significativa na ONU e em outros fóruns, a adoção de normas sobre segurança cibernética é recente, e muito ainda precisa ainda ser feito para ampliar sua

3 Radunovic, V; Grätz-Hoffmann, J; Maciel, M. Impact of Good Corporate Practices for Security of Digital Products on Global Cyber Stability. 13th International Conference on Cyber Conflict. Tallinn: NATO CCDCOE, 2021. Disponível em: <https://ccdcoe.org/uploads/2021/05/CyCon_2021_Radunovic_Gratz-Hoffmann_Maciel.pdf>

aceitação e implementação. O primeiro passo é tornar essas normas conhecidas do grande público. A tradução do relatório "Promovendo a Ciberestabilidade" para o português é um marco importante, que coloca essas normas ao alcance da população luso-falante.

A implementação de normas necessita de medidas concretas para lhes dar força. Domesticamente, estas medidas poderiam incluir a incorporação das normas na legislação nacional, na política nacional de segurança e defesa, e na doutrina militar. O apoio da sociedade civil e da academia também é fundamental para que normas ganhem raízes na sociedade.

O Brasil proporciona exemplos de como a colaboração entre diversos setores pode produzir princípios e normas de grande aceitação, que funcionam como lastro para o alinhamento de condutas e o desenvolvimento de normas em temas específicos. O Decálogo de Princípios para Governança e Uso da Internet no Brasil, aprovado em 2009 no âmbito do Comitê Gestor da Internet (CGI.br), foi uma iniciativa pioneira, que incentivou a convergência dos diversos setores participantes da governança da Internet no Brasil em torno de diretrizes fundamentais. O Decálogo também influenciou de maneira decisiva a redação do Marco Civil da Internet, uma lei que serve como pedra-angular para a construção do edifício regulatório em temas digitais no Brasil. No futuro, um grande avanço institucional seria implementar no Brasil um mecanismo permanente de engajamento multissetorial para abordar questões de estabilidade cibernética, uma das recomendações mais importantes feitas pelo presente relatório.

As oito normas elaboradas pela Comissão tratam de problemas centrais para a segurança e a estabilidade cibernéticas. O seu espectro de abrangência é amplo. Elas se debruçam tanto sobre temas que dizem respeito às camadas física e lógica da Internet, como também sobre questões relacionadas à cadeia de produção e desenvolvimento de produtos e serviços e à criação de uma cultura de cibersegurança.

O rol de normas aqui apresentadas é resultado não somente do debate entre os Comissários, mas é fruto do conhecimento produzido no âmbito de trabalhos de pesquisa que alimentaram as discussões da Comissão. A cada passo, processos de consulta foram conduzidos, tanto por meio de reuniões abertas presenciais que aconteceram à margem das reuniões da Comissão, como por meio de listas de discussão por e-mail, dedicadas a áreas temáticas

específicas. O objetivo foi não somente conduzir o processo de maneira aberta, mas também pôr o texto das normas à prova, por meio das críticas e sugestões recebidas.

Um enorme esforço de síntese foi necessário para comprimir o resultado de todas essas contribuições em normas sucintas, que pudessem ser facilmente apreendidas por quaisquer interessados. Felizmente, a riqueza das reflexões feitas ao longo dos anos não se perdeu: ela se encontra refletida nas seções iniciais do presente relatório e nos textos explicativos que acompanham as normas. Esse registro só foi possível graças ao trabalho incansável e minucioso do Secretariado que deu suporte à Comissão, sob a direção de Alexander Klimburg (The Hague Centre for Strategic Studies) e Bruce McConnell (EastWest Institute).

O rol de normas desenvolvidas pela Comissão é o ápice de um processo de colaboração multissetorial remarcável. Entretanto, essas normas não devem ser vistas como um ponto de chegada. Após a sua publicação, o conceito de ciberestabilidade continuou a evoluir, graças à emergência de diversas novas 'condições'[4], dentre as quais se encontram acordos recentes sobre normas, esforços de construção da confiança e de desenvolvimento de capacidade em temas de cibersegurança, e o lançamento de uma agenda de cooperação digital pelo Secretário Geral da ONU.

Em meio aos últimos desenvolvimentos, as normas elaboradas pela Comissão continuam atuais. Elas oferecem um ponto de atração gravitacional, contribuindo para uma órbita mais harmônica entre os diversos atores que fazem parte da constelação do ciberespaço. Sua força depende da ação conjunta de cada um de nós. A ciberestabilidade é um estado ideal, nunca plenamente satisfeito, que norteia o nosso caminhar e nossa responsabilidade compartilhada.

Marília Maciel
Pesquisadora sênior em políticas digitais da Diplo Foundation. Ex-presidente do Grupo Consultivo de Pesquisas em governança da Internet da Comissão Global sobre a Estabilidade do Ciberespaço.

4 Klimburg, A (Ed.) New Conditions and Constellations in Cyber. The Hague: The Hague Centre for Strategic Studies, 2021.

Comissão Global sobre a Estabilidade do Ciberespaço

Promovendo a Estabilidade no Ciberespaço para Construir a Paz e a Prosperidade

A Comissão Global sobre a Estabilidade do Ciberespaço (GCSC, na sigla em inglês) desenvolverá propostas de normas e políticas para melhorar a segurança e a estabilidade internacionais e orientar o comportamento responsável de atores estatais e não estatais no ciberespaço.

www.cyberstability.org | info@cyberstability.org | cyber@hcss.nl
@theGCSC

SECRETARIADO

Centro de Estudos Estratégicos de Haia (HCSS)
Intituto EastWest (EWI)

PARCEIROS

Governo dos Países Baixos
Corporação Microsoft
Agência de Segurança Cibernética de Singapura
Ministério das Relações Exteriores da França
Internet Society (ISOC)
Afilias

PATROCINADORES

Departamento Federal de Relações Exteriores da Suíça
GLOBSEC
Ministério das Relações Exteriores da Estônia
Ministério de Assuntos Internos e Comunicações do Japão

APOIADORES

Comissão da União Africana
Black Hat EUA
DEF CON
Delegação da União Europeia junto às Nações Unidas em Genebra
Fórum Global de Expertise Cibernética
Google
Prefeitura de Haia
Packet Clearing House
Universidade de Tel Aviv
Instituto das Nações Unidas para a Investigação sobre Desarmamento

Sumário

Carta dos Presidentes

por MICHAEL CHERTOFF e LATHA REDDY

O ciberespaço representa uma das maiores invenções da humanidade, reformulando relações pessoais, sociais, empresariais e políticas. Infelizmente, devido a ataques que ocorrem no e através do ciberespaço, é necessária uma ação urgente para garantir sua estabilidade. Este conceito de estabilidade do ciberespaço — como seu primo próximo, a estabilidade internacional — exige uma visão compartilhada, na qual todas as partes reconhecem que desacordos geopolíticos e mudanças que afetam o ciberespaço devem ser gerenciados em relativa paz, e que a estabilidade do ciberespaço deve ser assegurada.

A Comissão Global sobre a Estabilidade do Ciberespaço iniciou seus trabalhos convencida de que uma questão tradicionalmente reservada aos Estados — a paz e segurança internacionais — não poderia mais ser abordada sem envolver outras partes interessadas. O ciberespaço é um ambiente multissetorial: aqueles que constroem e gerenciam o ciberespaço, e aqueles que respondem a ataques no e através do ciberespaço, são tão suscetíveis de ser atores não estatais quanto agentes do governo. Nossos Comissários foram selecionados para refletir esta característica. Além de ex-altos funcionários do governo com experiência em questões de segurança internacional, nossas fileiras incluíram líderes reconhecidos das áreas de governança da Internet, das comunidades de direitos humanos e desenvolvimento, tecnologia e indústria. Juntos, nossos 28 Comissários de 16 países forneceram uma vasta gama de experiências e pontos de vista, e foram apoiados por comentários públicos em resposta à Comissão.

O relatório final da Comissão representa três anos de trabalho árduo. Reconhecemos com gratidão aqueles que tornaram isto possível: nossos Comissários, nossos conselheiros e pesquisadores (muitos deles voluntários), nossos apoiadores financeiros e o nosso Conselho de Administração. Por último, o nosso apreço dirige-se ao Secretariado, que não só geriu de forma habilidosa o processo, mas também foi fundamental para a criação da Comissão enquanto iniciativa da sociedade civil.

Ao longo dos seus trabalhos, a Comissão manteve-se consciente de outras iniciativas do ciberespaço, tanto no passado como no presente. Nosso relatório — Promovendo a Ciberestabilidade — complementa e reforça o trabalho dos outros, ao mesmo tempo em que fornece novas ideias para o avanço da estabilidade do ciberespaço.

Michael Chertoff
Co-presidente
Comissão Global sobre a Estabilidade do Ciberespaço

Latha Reddy
Co-presidente
Comissão Global sobre a Estabilidade do Ciberespaço

Sumário Executivo

Chegamos ao fim de um período de vinte e cinco anos de estabilidade estratégica e de relativa paz entre as grandes potências. Os conflitos entre Estados assumiram novas formas, e as atividades cibernéticas estão desempenhando um papel de liderança neste ambiente recentemente volátil. Ao longo da última década, o número e a sofisticação dos ataques cibernéticos por atores estatais e não estatais aumentaram, ameaçando assim a estabilidade do ciberespaço. Simplificando, as pessoas e as organizações podem não estar mais confiantes em sua capacidade de usar o ciberespaço com segurança, ou não ter certeza da disponibilidade e integridade dos serviços e das informações.

Neste contexto, a Comissão Global sobre a Estabilidade do Ciberespaço (GCSC) foi convocada para fazer recomendações para o avanço da ciberestabilidade. Começamos por identificar sete elementos de uma Estrutura de Ciberestabilidade. Essa estrutura inclui: (1) engajamento multissetorial; (2) princípios de ciberestabilidade; (3) desenvolvimento e implementação de normas voluntárias; (4) adesão ao direito internacional; (5) medidas de construção de confiança; (6) construção de capacidades; e (7) promulgação aberta e uso generalizado de normas técnicas que garantam que o ciberespaço seja resiliente. Após a definição desta estrutura, a Comissão analisou em profundidade três dos seus elementos: o engajamento multissetorial, os princípios e as normas.

Muitos acordos internacionais solicitam o engajamento multissetorial, mas este continua sendo controverso. Alguns ainda acreditam que garantir a segurança e a estabilidade internacionais é quase exclusivamente da responsabilidade dos Estados. Na prática, no entanto, o campo de batalha cibernético (ou seja, o ciberespaço) é projetado, implantado e operado principalmente por atores não estatais, e acreditamos que sua participação é necessária para garantir a estabilidade do ciberespaço. Além disso, a sua participação é inevitável, uma vez que os atores não estatais são muitas vezes os primeiros a responder a — e mesmo a atribuir — ataques cibernéticos.

A Comissão concluiu que estes atores não estatais não apenas são fundamentais para garantir a estabilidade do ciberespaço, mas deveriam também orientar-se por princípios e estar vinculados por normas. Os quatro princípios refletem esta visão, apelando a todas as partes para que sejam responsáveis, exerçam restrições, ajam e respeitem os direitos humanos:

- **Responsabilidade:** Todos são responsáveis por garantir a estabilidade do ciberespaço.
- **Restrição:** Nenhum ator estatal ou não estatal deve tomar medidas que prejudiquem a estabilidade do ciberespaço.
- **Obrigatoriedade de Ação:** Os atores estatais ou não estatais devem tomar medidas razoáveis e apropriadas para assegurar a estabilidade do ciberespaço.
- **Respeito aos Direitos Humanos:** Os esforços para garantir a estabilidade do ciberespaço devem respeitar os direitos humanos e o Estado de Direito.

Com base nesses princípios, e procurando complementar e não duplicar o trabalho de outros, a Comissão elaborou oito normas destinadas a garantir melhor a estabilidade do ciberespaço e dar resposta a preocupações técnicas ou a lacunas nas normas anteriormente estabelecidas:

1. Os atores estatais e não estatais não devem conduzir nem permitir conscientemente atividades que prejudiquem intencionalmente e substancialmente a disponibilidade geral ou a integridade do núcleo público da Internet e, por conseguinte, a estabilidade do ciberespaço.
2. Os atores estatais e não estatais não devem perseguir, apoiar ou permitir operações cibernéticas destinadas a disrupção da infraestrutura técnica essencial para eleições, referendos ou plebiscitos.
3. Os atores estatais e não estatais não devem adulterar produtos e serviços durante seu desenvolvimento e produção, nem permitir que sejam adulterados, se isso puder prejudicar substancialmente a estabilidade do ciberespaço.
4. Os atores estatais e não estatais não devem apropiar-se dos recursos das TIC do público em geral para sua utilização como *botnets* ou fins semelhantes.
5. Os Estados devem criar estruturas processualmente transparentes para avaliar se e quando devem divulgar vulnerabilidades ou falhas não conhecidas publicamente, e sobre as quais eles estejam cientes, nos sistemas e tecnologias da informação. A presunção padrão deve ser a favor da divulgação.
6. Desenvolvedores e produtores de produtos e serviços dos quais depende a estabilidade do ciberespaço devem (1) priorizar a segurança e a estabilidade, (2) tomar medidas razoáveis para garantir que seus produtos ou serviços estejam

livres de vulnerabilidades significativas e (3) tomar medidas para a mitigação oportuna das vulnerabilidades que serão posteriormente descobertas e ser transparentes sobre seu processo. Todos os atores têm o dever de compartilhar informações sobre vulnerabilidades, a fim de ajudar a prevenir ou mitigar atividades cibernéticas maliciosas.

7. Os Estados devem promulgar medidas apropriadas, incluindo leis e regulamentos, para assegurar a higiene cibernética básica.
8. Os atores não estatais não devem participar em operações cibernéticas ofensivas e os atores estatais devem prevenir essas atividades e responder caso elas ocorram.

Recomendações

Finalmente, reconhecendo tanto a importância do engajamento multissetorial quanto o fato de que declarar o comportamento como normativo não o torna assim, a Comissão faz seis recomendações que se focam no fortalecimento do modelo multissetorial, promovendo a adoção e implementação de normas e assegurando que aqueles que violam as normas sejam responsabilizados.

Concretamente, a Comissão recomenda que:

1. Os atores estatais e não estatais adotem e implementem normas que aumentem a estabilidade do ciberespaço, promovendo restrições e incentivando a tomada de ação.
2. Atores estatais e não estatais, em consonância com as suas responsabilidades e limitações, respondam de forma apropriada às violações das normas, garantindo que aqueles que violam as normas enfrentem consequências previsíveis e significativas.
3. Atores estatais e não estatais, incluindo instituições internacionais, intensifiquem os esforços para a formação de pessoal, desenvolvam e construam capacidades, promovam um entendimento comum da importância da estabilidade do ciberespaço, e levem em conta as necessidades díspares de diferentes partes.
4. Atores estatais e não estatais coletem, compartilhem, revisem e publiquem informações sobre violações de normas e o impacto de tais atividades.
5. Atores estatais e não estatais estabeleçam e apoiem Comunidades de Interesse para ajudar a garantir a estabilidade do ciberespaço.

6. Seja criado um mecanismo de engajamento multissetorial permanente para abordar questões de estabilidade, onde os Estados, o setor privado (incluindo a comunidade técnica) e a sociedade civil sejam adequadamente envolvidos e consultados.

A publicação deste relatório representa tanto um fim como um começo. A Comissão cumpriu o seu mandato. Para os membros e apoiadores da GCSC, no entanto, bem como para todos aqueles que apoiam seus objetivos, o trabalho árduo necessário para implementar esses princípios, normas e recomendações está apenas começando. É preciso começar, uma vez que os benefícios do ciberespaço serão perdidos se a sua estabilidade não for assegurada.


EUROPE

I Introdução

A evolução digital e o ciberespaço transformaram drasticamente a existência humana.[1] A capacidade de digitalizar, armazenar, analisar e transportar dados ao redor do globo teve efeitos profundos em todos os setores da sociedade, e mudou a maneira como conduzimos assuntos pessoais, empresariais e políticos. Hoje, aproximadamente metade da população mundial está on-line[2] e este número está aumentando rapidamente. Mas mesmo aqueles que não estão pessoalmente conectados ao ciberespaço são afetados por seu alcance, uma vez que as entidades das quais dependem para fornecer bens e serviços muitas vezes usam o ciberespaço para comunicações, logística e finanças.

Os benefícios do ciberespaço — e a necessidade de garantir sua estabilidade — têm sido frequentemente discutidos, assim como os seus desafios. Mais notavelmente, o ciberespaço pode suportar tanto propósitos nobres como ignóbeis. Por exemplo, a conectividade global, o anonimato e a falta de rastreabilidade permitem que indivíduos e máquinas se conectem a dados e sistemas sem afirmar sua identidade, mas os criminosos também podem se aproveitar desses atributos para cometer crimes impunemente. Como resultado, governos, empresas e pessoas ao redor do mundo confrontam-se com

1 O "ciberespaço" foi definido de várias maneiras. <https://en.wikipedia.org/wiki/Cyberspace>. A definição do dicionário é "um sistema eletrônico que permite que usuários de computador em todo o mundo se comuniquem uns com os outros ou acessem informações para qualquer finalidade". <https://dictionary.cambridge.org/us/dictionary/english/cyberspace>. De acordo com o Reino Unido, "Ciberespaço é o termo usado para descrever o meio eletrônico de redes digitais usado para armazenar, modificar e comunicar informações. Inclui a Internet, mas também outros sistemas de informação que apoiam empresas, infraestruturas e serviços." <https://www.cpni.gov.uk/cyber>. Como tal, é indiscutivelmente mais abrangente do que a Internet, que é descrita em termos populares como um "sistema global de redes de computadores interligados que usam o conjunto de protocolos de Internet (TCP/IP) para ligar dispositivos em todo o mundo." Ver <https://en.wikipedia.org/wiki/Internet>. Ver também União Internacional de Telecomunicações, "Defining the Internet," documento para discussão (maio 2013),<https://www.itu.int/dms_pub/itu-s/md/13/wtpf13/inf/S13-WTPF13-INF-0008%21%21MSW-E.docx>

2 "Internet Usage Statistics," Internet World Stats, última modificação em 4 de outubro de 2019, <https://internetworldstats.com/stats.htm>

dilemas. Os governos estão interessados em proteger o ciberespaço, prestar serviços públicos e promover outras atividades importantes (por exemplo, educação e operações bancárias on-line), mas também estão interessados em promover interesses de segurança nacional, incluindo a aplicação da lei, inteligência e capacidades militares. As empresas, preocupadas em proteger seus clientes, reputações e lucros, encontram-se sob ataque, investigando atividades maliciosas e/ou sujeitas a solicitações governamentais de dados. As pessoas — estejam elas conectadas ou não — dependem cada vez mais e adotam a tecnologia digital, mas estão preocupadas com sua disponibilidade e integridade contínuas. Ao longo da última década, o número e a sofisticação dos ciberataques aumentaram, incluindo ataques a sistemas governamentais e infraestruturas críticas.[3] Assim sendo, nem o status quo nem as tendências observáveis são encorajadores.

Os ataques cibernéticos, conduzidos por atores estatais e não estatais, deixam claro que o mundo precisa de uma Estrutura de Ciberestabilidade . Essa estrutura servirá para reduzir o potencial de disrupções significativas do ciberespaço que prejudicarão seus benefícios e reduzirão o bem-estar das pessoas, incluindo os seus direitos e liberdades. Claramente, produtos e serviços bem projetados e construídos, bem geridos por profissionais de TI e usuários de computadores, irão aumentar a segurança e a estabilidade, assim como produtos e serviços concebidos de forma precária ou negligente, ou práticas operacionais precárias ou negligentes, irão prejudicá-los. Mas melhorar desenvolvimentos e operações não será suficiente, especialmente quando atores estatais e não estatais veem o ciberespaço como um campo de batalha onde se podem alcançar vantagens políticas, militares ou econômicas. Um agressor persistente pode derrotar medidas de segurança, dando origem ao ditado de que "o ataque derrota

3 Centro de Estudos Estratégicos e Internacionais (CSIS), "Significant Cyber Incidents Since 2006", <https://csis-website-prod.s3.amazonaws.com/s3fs-public/200626_Cyber_Events.pdf>; Louis Marinos and Marco Lourenço, ed., "ENISA Threat Landscape Report 2018", ENISA (janeiro de 2019), <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>; Abhishek Agrawal et al., "Microsoft Security Intelligence Report", Vol. 24 (dezembro de 2018), <https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original>; Nações Unidas , Assembleia Geral, "Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General, A/74/120" (24 junho de 2019), <https://undocs.org/A/74/120>

a defesa na Internet" e criando instabilidade.[4] Assim, é importante concentrar-se não apenas na tecnologia, mas nos comportamentos: como encorajar todos os atores a se comportarem de forma responsável que aumente — e não ameace — a estabilidade do ciberespaço?

Para ajudar a responder a esta pergunta, várias entidades governamentais e não governamentais apoiaram a criação da Comissão Global sobre a Estabilidade do Ciberespaço (GCSC, na sigla em inglês),[5] observando que:

> *Chegamos ao fim de um período de vinte e cinco anos de estabilidade estratégica e de relativa paz entre as grandes potências. Os conflitos entre Estados assumirão novas formas e as atividades cibernéticas poderão desempenhar um papel de liderança neste ambiente recentemente volátil, aumentando assim o risco de minar a utilização pacífica do ciberespaço para facilitar o crescimento econômico e a expansão de liberdades individuais.*
> *A fim de contrariar esses desenvolvimentos, a Comissão Global sobre a Estabilidade do Ciberespaço desenvolverá propostas de normas e políticas para melhorar a segurança e a estabilidade internacionais e orientar o comportamento estatal e não estatal responsável no ciberespaço. A GCSC envolverá toda a gama de partes interessadas para desenvolver entendimentos compartilhados, e seu trabalho promoverá a ciberestabilidade, apoiando o intercâmbio de informações e a construção de capacidades, pesquisa básica e ativismo.*[6]

Nomeadamente, a própria Comissão é multissetorial e global, uma vez que é composta por indivíduos com conhecimentos e históricos diversos. Alguns Comissários atuaram no governo e participaram em negociações bilaterais e multilaterais sobre questões cibernéticas,

---

4 Ver, por exemplo, P.W. Singer and Allan Friedman, "The Cult of the Cyber Offensive," Foreign Policy (15 de janeiro de 2014), https://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/ ; Fórum Econômico Mundial (WEF), "The Global Risks Report 2019", (2019), <https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf>

5 Para mais informações sobre a GCSC, consulte o Apêndice C: História, Objetivos e Processos da GCSC.

6 Comissão Global sobre a Estabilidade do Ciberespaço, <https://cyberstability.org/>

enquanto outros têm experiência na construção, manutenção e proteção da própria Internet. Outros representaram a sociedade civil.

O trabalho da Comissão não existe em um vácuo e a GCSC, reconhecendo que muitas outras instituições e processos (tanto passados como atuais) compartilham o seu interesse pela estabilidade do ciberespaço, procurou não duplicar outros trabalhos. Em vez disso, a GCSC tenta apoiar-se sobre outros processos multissetoriais e governamentais e influenciar trabalhso futuros. Esses processos incluem o trabalho fundamental e contínuo do Grupo de Especialistas Governamentais das Nações Unidas (GGE, na sigla em inglês, da ONU),[7] o trabalho do Grupo de Trabalho Aberto (OEWG, na sigla em inglês, da ONU), bem como os esforços do Fórum Global de Expertise Cibernética (GFCE, na sigla em inglês),[8] da Cúpula Mundial sobre a Sociedade da Informação (CMSI), da Comissão Global de Governança da Internet (Comissão Bildt), do Fórum de Governança da Internet (IGF, na sigla em inglês), Conferência Global sobre Espaço Cibernético (GCCS/Processo de Londres), da Iniciativa NetMundial, Organização para a Segurança e Cooperação na Europa (OSCE), da Comissão da União Africana (AUC, na sigla em inglês), da Carta de Confiança, do Acordo Tecnológico de Segurança Cibernética, do Programa de Haia para Normas Cibernéticas, do Instituto das Nações Unidas para a Investigação sobre Desarmamento (UNIDIR, na sigla em inglês), do Chamado de Paris para a Confiança e Segurança no Ciberespaço ("Paris Call", em inglês) e do Painel de Alto Nível sobre Cooperação Digital do Secretário-Geral da ONU. Os trabalhos da Comissão foram igualmente informados por pesquisa encomendada e pedidos de comentários públicos.

---

7 Em uma importante resolução de 2015, a Assembleia Geral das Nações Unidas confirmou por unanimidade a conclusão do GGE da ONU. Ver Resolução 70/237 da Assembleia Geral, da Resolução adotada pela Assembleia Geral em 23 de dezembro de 2015 [sobre o relatório do Primeiro Comitê (A/70/455), <https://undocs.org/en/A/RES/70/237>]. Assim, o direito internacional e, em particular, a Carta das Nações Unidas estabelecem um quadro exclusivo de resposta internacional a atos hostis que também se aplica às operações cibernéticas. O nosso trabalho baseia-se no acordo de todos os Estados na Assembleia Geral da ONU de 2015 para serem orientados por normas de comportamento responsável para aumentar a estabilidade e a segurança no uso das TICs e para cumprir os seus compromissos ao abrigo do direito internacional para a devida diligência e cooperação.

8 O GFCE tem estado particularmente ativo na contrução de capacidades. Ver, por exemplo, "Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building", Fórum Global de Expertise Cibernética (24 de novembro de 2017), <https://thegfce.org/wp-content/uploads/2020/04/DelhiCommunique.pdf>

Alguns dos esforços mencionados centraram-se, em parte, na estabilidade do ciberespaço, e preocuparam-se com o fato da estabilidade e a governança do ciberespaço estrem indissociavelmente ligadas. Ou seja, na ausência de um modelo de governança robusto, a sociedade carece das interações e dos processos de tomada de decisão necessários para garantir a estabilidade. Por exemplo, a Comissão Bildt propôs um pacto social multissetorial para a privacidade e segurança digitais "entre os cidadãos e os seus representantes eleitos, o poder judicial, as agências de aplicação da lei e de inteligência, as empresas, a sociedade civil e a comunidade técnica da Internet, com o objetivo de restaurar a confiança e aumentar a confiabilidade na Internet."[9]

Elogiamos esses esforços anteriores no desenvolvimento de princípios, regras e normas para aplicar ao comportamento no novo domínio turbulento do ciberespaço e acreditamos que uma estrutura abrangente é necessária para aumentar a estabilidade do ciberespaço. O registro histórico mostra que sociedades e governos podem, em alguns casos, levar décadas para desenvolver estruturas de governança internacionais amplas e formais para novas tecnologias disruptivas importantes.[10] O surgimento do ciberespaço como uma dimensão crucial da interdependência econômica, social e de segurança global data apenas do final da década de 1990, quando a World Wide Web começou a ser amplamente utilizada. Assim, os processos evolutivos de governança encontram-se numa fase inicial em que coexistem áreas de coerência e incoerência normativa.[11] Por exemplo, enquanto normas e instituições relacionadas ao Sistema de Nomes de Domínio estão bem desenvolvidas, existem grandes áreas de desacordo entre os Estados e entre as empresas relacionadas à regulação de conteúdo. Por vezes, os atores estatais e não estatais aplicam normas de outros

9 Comissão Global de Governança da Internet, "One Internet (2016)", p. IX, <https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf> "Apelamos aos governos, empresas privadas, sociedade civil, comunidade técnica e indivíduos juntos para criar um novo pacto social para a era digital".

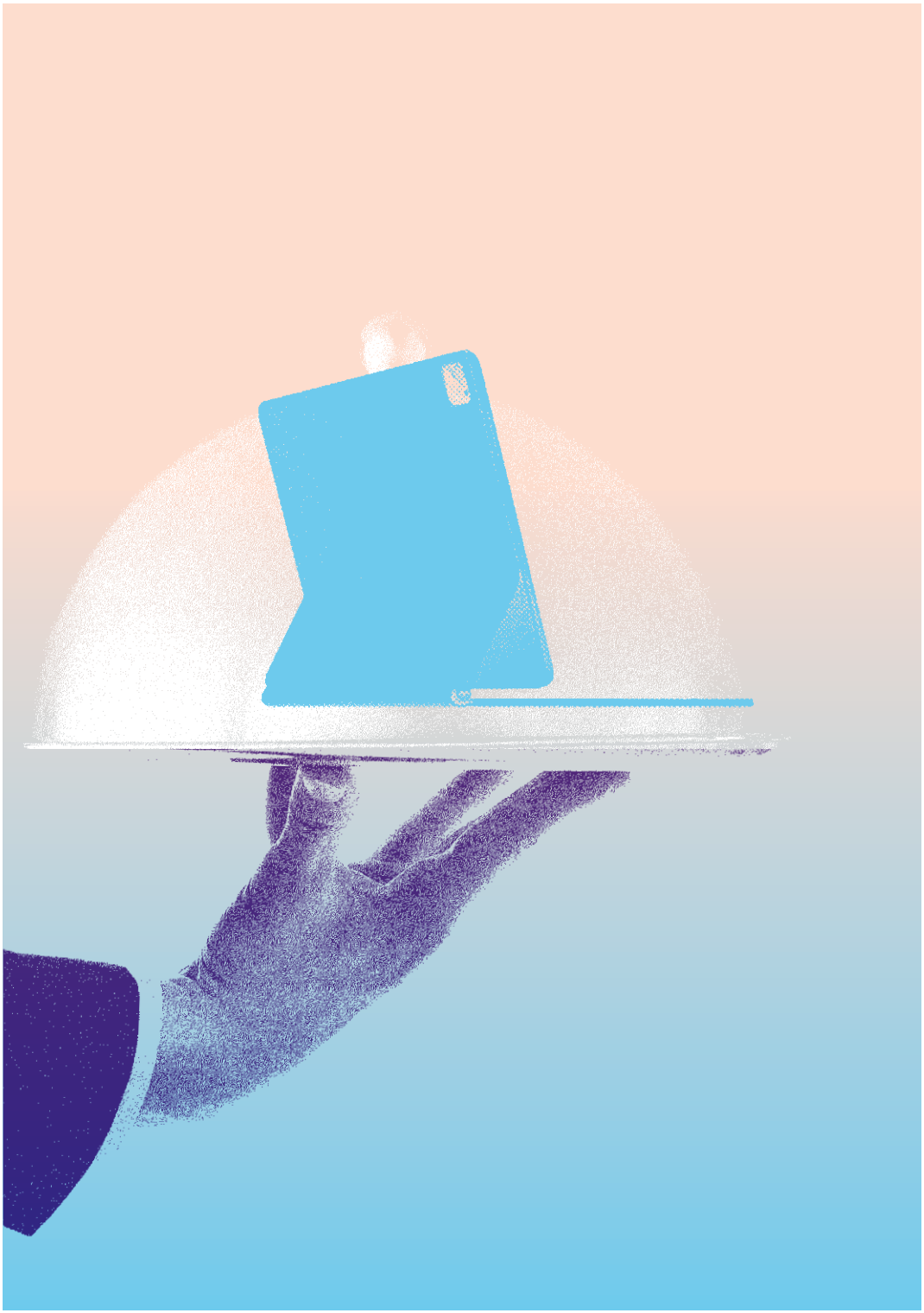
10 Talvez o exemplo mais pertinente de uma estrutura de governança deste tipo esteja relacionado com as armas nucleares, que levaram tempo e esforços significativos para se estabelecer. Mesmo agora, 60 anos depois do Tratado de Não-Proliferação de Armas Nucleares (TNP), a governança das armas nucleares continua sendo uma preocupação de segurança.

11 Esta fase inicial tem sido chamada de "complexo de regime". Ver Joseph Nye, "The Regime Complex for Managing Complex Global Cyber Activities," Comissão Global de Governança da Internet, No. 1 (maio de 2014), <https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf>

regimes como a propriedade intelectual e o comércio e, cada vez mais, as empresas privadas estão estabelecendo normas.[12] O objetivo da nossa Comissão não é resolver estas várias questões da governança, mas colocá-las em uma estrutura geral para garantir a estabilidade do ciberespaço.

Observamos também que aqueles que se preocupam com a estabilidade do ciberespaço têm lutado para acompanhar aqueles que procuram miná-lo, bem como acompanhar os desenvolvimentos tecnológicos e a evolução dos conflitos geopolíticos. Parte do desafio é que o ciberespaço transformou a forma como os atores buscam seus objetivos políticos e militares; com baixas barreiras à entrada, é menos difícil tornar-se uma potência cibernética do que uma potência militar tradicional. Além disso, com a nova tecnologia em suas caixas de ferramentas, alguns estão hesitantes em adotar restrições, especialmente se essas restrições não forem amplamente honradas. O que é necessário é uma Estrutura de Ciberestabilidade abrangente para a comunidade internacional, que promova a estabilidade do ciberespaço, mas que continue sendo útil à medida que o ritmo das mudanças tecnológicas continue a aumentar. Começamos, portanto, por definir o objetivo central: proteger a estabilidade do ciberespaço.

12 Ver, por exemplo, as normas desenvolvidas pela Sociedade da Internet (ISOC) e Microsoft: "Mutually Agreed Norms for Routing Security (MANRS)," Sociedade da Internet (2014), <https://www.manrs.org/>; Angela McKay et al., "International Cybersecurity Norms Reducing Conflict in an Internet-dependent World", Microsoft (dezembro de 2014), <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA>; and Scott Charney et al., "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms", Microsoft (junho de 2016), <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8>



II O que significa a estabilidade do ciberespaço?

DEFINIÇÃO: A estabilidade do ciberespaço significa que todos podem estar razoavelmente confiantes na sua capacidade de utilizar o ciberespaço com segurança, onde a disponibilidade e integridade dos serviços e informações fornecidos no ciberespaço e através do ciberespaço são geralmente asseguradas, onde a mudança é gerida em relativa paz e onde as tensões são resolvidas de forma não escalonada.

Embora a definição da Comissão se baseie na definição padrão de "estabilidade"[13], essa definição contém dois matizes. Primeiro, existe uma referência à confiança do usuário. A confiança é importante porque as decisões humanas podem basear-se em percepções, não apenas em fatos, e se alguém percebe uma falta de estabilidade, tais pessoas podem relutar em usar o ciberespaço e obter seus benefícios. A título de exemplo, o uso do ciberespaço pode simplificar os processos e torná-los mais eficientes, sugerindo assim que certas funções (por exemplo. acesso a serviços governamentais, serviços bancários on-line) poderiam se beneficiar das potencialidades do ciberespaço. Mas se tais sistemas não são confiáveis — ou se há uma percepção de que tais sistemas não são confiáveis — seu uso será limitado, e os benefícios da tecnologia serão perdidos.

13 "Estabilidade" é definido como "o estado de ser estável." <https://www.lexico.com/en/definition/stability>. Estável significa (1) não suscetível de ceder ou virar; firmemente fixado; (2) não suscetível de mudar ou falhar; firmemente estabelecido; e (3) não suscetível de sofrer alterações físicas. Ver <https://en.oxforddictionaries.com/definition/stability>. Nas Relações Internacionais, uma das definições mais consistentes do termo "estabilidade internacional" tem sido "a probabilidade de que o sistema [internacional] retenha todas as suas características essenciais; que nenhuma nação se torne dominante; que a maioria dos seus membros continue a sobreviver; e que não ocorra uma guerra em larga escala". Karl W. Deutsch e J. David Singer, "Multipolar Power Systems and International Stability", World Politics, Vol. 16, Nº 3 (abril de 1964): 390-406, <http://users.metu.edu.tr/utuba/Deutsch.pdf>

Segundo, deve-se lembrar de que o ciberespaço é um domínio em constante mudança. Há mudanças na tecnologia, nos modelos de negócios, na funcionalidade e nas expectativas da sociedade sobre o papel da tecnologia na vida diária. Assim, ao contrário da definição do dicionário de "estabilidade", que inclui "retornar a uma condição original", o que precisamos são mecanismos ágeis para garantir a estabilidade do ciberespaço à medida que as tecnologias evoluem. Simplificando, todos devem permanecer confiantes na disponibilidade e integridade do ciberespaço, mesmo que ele — e o mundo ao seu redor — mude.

III A estrutura de ciberestabilidade da GCSC

Para enfrentar os desafios descritos acima, a GCSC, assim como outros o fizeram[14], propõe uma Estrutura de Ciberestabilidade abrangente. Essa estrutura inclui (1) engajamento multissetorial; (2) princípios de ciberestabilidade; (3) desenvolvimento e implementação de normas voluntárias; (4) adesão ao direito internacional; (5) medidas de construção de confiança; (6) construção de capacidades; e (7) promulgação aberta e uso generalizado de normas técnicas que garantam que o ciberespaço seja resiliente. Os esforços da GCSC concentraram-se principalmente em três desses itens — abordagem multissetorial, princípios e normas — que são tratados nas Seções 4, 5 e 6, respectivamente. Em relação às normas, nos concentramos não apenas no seu desenvolvimento, mas nas questões mais difíceis de adoção, implementação e *accountability** dos infratores.

14 Ver, por exemplo, A Era da Interdependência Digital: Relatório do Painel de Alto Nível do Secretário-Geral das Nações Unidas sobre a Cooperação Digital (junho de 2019), p. 29, <https://cgi.br/media/docs/publicacoes/1/20200901150023/CadernoCGIbr_A_era_da_interdependencia_digital.pdf>. "Recomendamos o desenvolvimento de um Compromisso Global sobre a Confiança e Segurança Digital para moldar uma visão compartilhada, identificar atributos de estabilidade digital, elucidar e fortalecer a implementação de normas para usos responsáveis da tecnologia, e propor prioridades de ação".

*Para fins desta publicação, optou-se por manter a palavra "accountability" no original em inglês, para maior consistência de sentido.

IV Engajamento multissetorial

Apesar de uma infinidade de acordos internacionais entre os Estados citarem a importância de uma abordagem multissetorial, esta continua sendo controversa. Para alguns, o debate é filosófico e centra-se nos papéis comparativos dos atores estatais e não estatais na política tecnológica e nos assuntos internacionais. Para outros, os processos multissetoriais são práticos, sustentando que os Estados agindo sozinhos ou apenas com um mínimo de contribuição não estatal não podem garantir a estabilidade do ciberespaço.[15] Concordamos com esta última visão.

Este debate sobre os méritos do engajamento multissetorial dura há décadas. Muitas vezes, a questão surgiu no contexto da gestão dos recursos da Internet, mas a questão das normas e da segurança nacional também foi levantada. Por exemplo, durante a segunda fase da Cúpula Mundial da ONU sobre a Sociedade da Informação (CMSI), o Grupo de Trabalho das Nações Unidas sobre Governança da Internet (WGIG, na sigla em inglês) rejeitou o conceito de liderança de uma única parte interessada. Em vez disso, concluiu que a Internet é demasiado grande para ser gerida por um grupo de partes interessadas ou apenas por uma organização e propôs uma abordagem multissetorial. Assim, em 2005, os Chefes de Estado na Agenda da Túnis da CMSI declararam que "Uma definição de

15 "A definição da CMSI (2005) introduziu o conceito dos 'respectivos papéis' e a filosofia da 'partilha'. A Declaração NETMundial (2014) definiu elementos-chave como de baixo para cima, abertura, transparência, inclusão e base dos direitos humanos. Em outras palavras, temos algumas diretrizes gerais para uma abordagem multissetorial, mas não temos um único modelo multissetorial. Até agora, surgiram dois modelos multissetoriais diferentes: o modelo consultativo e o modelo colaborativo. " Wolfgang Kleinwächter, "Towards a Holistic Approach for Internet Related Public Policy Making," Comissão Global sobre a Estabilidade do Ciberespaço (janeiro de 2018), <https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf>. Para uma discussão adicional sobre modelos multissetoriais, ver Virgilio Almeida et al., "The Origin and Evolution of Multistakeholder Models", IEEE Internet Computing, Vol. 19 (janeiro-fevereiro de 2015): 74-79, <https://www.computer.org/csdl/magazine/ic/2015/01/mic2015010074/13rRUNvya5I>

trabalho da governança da Internet é odesenvolvimento e a aplicação por parte dos governos, do setor privado e da sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos decisórios e programas compartilhados que dão forma à evolução e uso da Internet."[16]

Esta visão foi reafirmada dez anos mais tarde na Reunião de Alto Nível da Assembleia Geral das Nações Unidas sobre a revisão global da implementação dos resultados da CMSI, também indicada na Resolução 70/125 (2015) da ONU:

> *Reafirmamos, além disso, o valor e os princípios da cooperação e do engajamento multissetorial que caracterizaram a Cúpula Mundial sobre a Sociedade da Informação desde o seu início, reconhecendo que a participação efetiva, a parceria e a cooperação dos governos, do setor privado, da sociedade civil, das organizações internacionais, das comunidades técnicas e acadêmicas e de todas as outras partes interessadas relevantes, no âmbito das respectivas funções e responsabilidades, especialmente com uma representação equilibrada dos países em desenvolvimento, têm sido e continuam sendo vitais para o desenvolvimento da sociedade da informação.* [17]

Mais uma vez, a declaração foi além da gestão de recursos críticos da Internet e diretamente para o centro das questões de segurança nacional:

> *Reconhecemos o papel de liderança dos governos em questões de segurança cibernética relacionadas com a segurança nacional. Reconhecemos ainda os papéis e as importantes contribuições de todas as partes interessadas, em suas respectivas funções e responsabilidades.* [18]

---

16 Agenda de Túnis para a Sociedade da Informação, p.78, disponível em: <https://cgi.br/media/docs/publicacoes/1/CadernosCGIbr_DocumentosCMSI.pdf>

17 Ver Resolução 70/125 da Assembleia Geral das Nações Unidas, Documento Final da reunião de alto nível da Assembleia Geral sobre a revisão geral da implementação dos resultados da Cúpula Mundial da Sociedade da Informação, A/RES/70/125 (16 de dezembro de 2015), Parágrafo 3, <https://undocs.org/A/RES/70/125>

18 Id., Parágrafo 50.

No que diz respeito especificamente às normas, o Grupo dos Oito (G8) declarou em 2011 que:

> *A segurança de redes e serviços na Internet é uma questão multissetorial. Requer coordenação entre governos, organizações regionais e internacionais, setor privado, [e] sociedade civil... Os governos têm um papel a desempenhar, informados por uma gama completa de partes interessadas, ajudando a desenvolver normas de comportamento e abordagens comuns no uso do ciberespaço.* [19]

Dois anos mais tarde, em 2013, o Grupo de Especialistas Governamentais das Nações Unidas (GGE da ONU) publicou seu Relatório Sobre Avanços no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional. Em uma seção intitulada "Promoção da cooperação para alcançar um ambiente pacífico, seguro, resiliente e aberto para as tecnologias de informação e comunicação", o GGE da ONU observou que "embora os Estados devam liderar a resolução desses desafios, uma participação apropriada do setor privado e da sociedade civil melhoraria a cooperação." [20] O relatório continuou afirmando, em uma seção intitulada "Recomendações sobre normas, regras e princípios de comportamento estatal responsável", que:

> *Os Estados-Membros devem considerar a melhor forma de cooperar para implementar as normas e princípios de comportamento responsável acima referidos, incluindo o papel que o setor privado e as organizações da sociedade civil podem desempenhar.* [21]

---

19 Grupo dos Oito, "G8 Declaration: Renewed Commitment for Freedom and Democracy", Cúpula do G8 em Deauville (27 de maio de 2011), Parágrafo 17, <http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html>.

20 Assembleia Geral das Nações Unidas, Relatório do Grupo de Especialistas Governamentais sobre Desenvolvimentos no Domínio da Informação e Telecomunicações no Contexto da Segurança Internacional, A/68/98 (24 de junho de 2013), p.7, § 12, <https://undocs.org/A/68/98> (doravante, Relatório 2013 do GGE da ONU).

21 Id., p. 8, § 25.

Estas posições foram reafirmadas no relatório de 2015 do GGE da ONU, onde foi declarado que:

> *Embora os Estados tenham a principal responsabilidade pela manutenção de um ambiente de TIC seguro e pacífico, uma cooperação internacional eficaz se beneficiaria da identificação de mecanismos de participação do setor privado, do meio acadêmico e das organizações da sociedade civil, conforme o caso.* [22]

Esta declaração foi repetida em uma resolução da Assembleia Geral de 2018 sobre a Promoção do comportamento responsável dos Estados no ciberespaço no contexto da segurança internacional. [23] Outros acordos internacionais expressam claramente o mesmo sentimento; por exemplo, o Chamado de Paris (Paris Call, em inglês) declarou: "Reconhecemos a necessidade de uma abordagem consolidada com várias partes interessadas e de esforços adicionais para reduzir os riscos para a estabilidade do ciberespaço e para aumentar a segurança, a capacidade e confiança." [24]

---

22 Assembleia Geral das Nações Unidas, Relatório do Grupo de Especialistas Governamentais sobre Desenvolvimentos no Domínio da Informação e Telecomunicações no Contexto da Segurança Internacional, A/70/174 (22 de julho 2015), p.13, parágrafo 31, <https://undocs.org/en/A/70/174>, (doravante, Relatório 2015 do GGE da ONU).

23 Assembleia Geral das Nações Unidas, Resolução 73/266, Promovendo o comportamento responsável dos Estados no ciberespaço no contexto da segurança internacional, A/RES/73/266 (22 December 2018), <https://undocs.org/A/RES/73/266>

24 Ministério para a Europa e Relações Exteriores da França, "Paris Call for Trust and Security in Cyberspace" (11 de novembro de 2018), <https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918>. Ver também, NETMundial, "NetMundial Multistakeholder Statement" (24 de abril de 2014), <https://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>. [Declaração Multissetorial do NETmundial, disponível em: <https://cgi.br/media/docs/publicacoes/1/16570020190607-CadernosCGIbr_DeclaracaoNETmundial.pdf>

Mais recentemente, em junho de 2019, o Painel de Alto Nível sobre Cooperação Digital do Secretário-Geral da ONU, em seu relatório, A Era da Interdependência Digital, declarou:

> *Uma cooperação digital eficaz exige que o multilateralismo, apesar das atuais tensões, seja reforçado. Também exige que o multilateralismo seja complementado pelo multissetorialismo - cooperação que envolve não apenas os governos, mas um espectro muito mais diversificado de outros setores, como a sociedade civil, a academia, tecnologistas e o setor privado.* [25]

Embora a ideia de uma abordagem multissetorial tenha provado ser bem sucedida, ela não é universalmente apoiada. Alguns governos continuam acreditando que garantir a segurança e a estabilidade internacionais é quase que exclusivamente da responsabilidade dos Estados. Esta visão mais tradicional da segurança nasce da noção de que os Estados têm a responsabilidade de proteger os seus cidadãos dos ataques através de meios vigorosos, uma ideia refletida nas responsabilidades do Conselho de Segurança das Nações Unidas, tal como codificado no artigo 24 da Carta das Nações Unidas. [26] Esta linha de pensamento pode também ser reforçada pela experiência passada, porque, no domínio físico, os governos não só gozavam de um monopólio sobre o uso legítimo da força, mas também estavam no controle de armas de nível militar (por exemplo, aviões, tanques) usadas para atacar e defender esse domínio.

Na prática, o campo de batalha cibernético (ou seja, o ciberespaço) é projetado, implantado e operado principalmente pelo setor privado. Os governos não são, apesar de suas responsabilidades específicas, os protetores exclusivos deste domínio. Mesmo que os governos mantenham um monopólio de direito sobre o uso legítimo da força no ciberespaço, eles já não têm um monopólio prático de atacar e proteger este domínio, nem podem impedir a proliferação e a utilização de armas cibernéticas poderosas. Pelo contrário, a comunidade técnica, a sociedade civil e os indivíduos também

25 A Era da Interdepencia Digital, p. 26, <https://cgi.br/media/docs/publicacoes/1/20200901150023/CadernoCGIbr_A_era_da_interdependencia_digital.pdf>

26 Carta das Nações Unidas, "Chapter V - The Security Council," Repertório de prática dos órgãos das Nações Unidas, <https://legal.un.org/repertory/art24.shtml>

desempenham um papel importante na proteção do ciberespaço, incluindo a promulgação de práticas. Portanto, a abordagem multissetorial é necessária para melhorar os resultados e garantir que as normas e políticas de apoio à estabilidade do ciberespaço sejam bem formadas e evitem consequências indesejadas.

Igualmente importante, mesmo que os Estados desejem seguir sozinhos, não poderão. A participação de atores não estatais em questões que afetam a estabilidade do ciberespaço é inevitável. Por exemplo, muitos membros do setor privado e da comunidade técnica podem ser responsáveis por protocolos e serviços críticos, e podem proteger Estados que usam seus produtos comerciais e de código aberto. Além disso, até mesmo a investigação e atribuição de ataques, papel tradicional e de prerrogativa política dos governos, não é mais sua única área de conhecimento e responsabilidade; alguns ataques estatais notáveis têm sido identificados e divulgados por entidades não governamentais. Em suma, embora os Estados tenham um papel único a desempenhar durante e após um ataque (incluindo atividades de aplicação da lei e/ou ações diplomáticas ou outras ações do Estado), eles não têm monopólio de pesquisa e atribuição, nem podem efetivamente excluir atores não estatais. Como resultado, desenvolver normas e políticas bem sucedidas para o ciberespaço — e garantir a sua adesão — exige a participação, e é de responsabilidade, de todas as partes interessadas, e os governos devem concentrar-se na criação de mecanismos que incorporem efetivamente a participação do setor privado, da comunidade técnica, academia, e outros representantes da sociedade civil. Foi exatamente isso que muitos governos pediram.

V Princípios

O comportamento normativo deriva de valores. Declarar esses valores, sejam eles relacionados a responsabilidades individuais, responsabilidades estatais ou direitos humanos fundamentais, deve, portanto, ser o nosso ponto de partida. De fato, valores diferentes podem dificultar a obtenção de consensos, bem como resultar em diferentes interpretações e implementações de acordos internacionais por parte de países ou regiões. Isto não significa que um acordo sobre princípios seja necessário para que se obtenha progresso; às vezes, as partes concordam em comportamentos aceitáveis, mesmo que seus motivos para fazê-lo sejam diferentes. Mas os princípios comuns e a interdependência podem levar a compromissos mais profundos e reduzir o risco de futuras discordâncias ou conflitos. Por isso, é importante que as partes mantenham discussões francas sobre os princípios de alto nível que orientam o seu pensamento e dos quais emanam as normas.

Os quatro princípios a seguir são fundamentais para garantir a estabilidade do ciberespaço:

1. **Responsabilidade:** Todos são responsáveis por garantir a estabilidade do ciberespaço.
2. **Restrição:** Nenhum ator estatal ou não estatal deve tomar medidas que prejudiquem a estabilidade do ciberespaço.
3. **Obrigatoriedade de Ação:** Os atores estatais ou não estatais devem tomar medidas razoáveis e apropriadas para assegurar a estabilidade do ciberespaço.
4. **Respeito aos Direitos Humanos:** Os esforços para garantir a estabilidade do ciberespaço devem respeitar os direitos humanos e o Estado de Direito.

A. Princípio da Responsabilidade

O primeiro princípio fala da natureza descentralizada e distribuída do ciberespaço. Reafirma a necessidade de uma abordagem multissetorial para garantir a estabilidade do ciberespaço e, nomeadamente, expande as "partes interessadas" para incluir todos os indivíduos. Cada indivíduo tem responsabilidades, pessoais e/ou profissionais, de assegurar a estabilidade do ciberespaço. Embora possa ser óbvio que os responsáveis pelas políticas cibernéticas do

governo e os funcionários que gerenciam os serviços de nuvem têm um papel a desempenhar, cada indivíduo conectado ao ciberespaço deve fazer esforços razoáveis para garantir que seus próprios dispositivos não sejam comprometidos e, talvez, usados em ataques. Mesmo aqueles que não estão conectados à Internet podem depender de suas capacidades para receber bens e serviços, e também têm interesse em assegurar que a política do ciberespaço esteja sendo tratada adequadamente em suas comunidades.

B. Princípio da Restrição

O segundo princípio contém um requisito geral de restrição. Para os Estados, isto é coerente com as resoluções da Assembleia Geral das Nações Unidas (AGNU) de 2018 sobre o comportamento responsável do Estado no ciberespaço[27] e com o relatório do GGE da ONU, de 2015, que observa que "Os Estados, em consonância com os propósitos das Nações Unidas, incluindo a manutenção da paz e segurança internacionais, devem ... evitar práticas no domínio das TIC que sejam consideradas prejudiciais ou que possam colocar em risco a paz e a segurança internacionais..."[28] Mas não se trata apenas de Estados, já que os atores não estatais também podem se envolver em ações, como o haqueamento de seus agressores, que também podem minar a estabilidade do ciberespaço.

C. O princípio da Obrigatoriedade da Ação

O terceiro princípio contém um requisito geral de tomar ações afirmativas para preservar a estabilidade do ciberespaço. Ao agir, os Estados devem tomar cuidado para evitar tensões inadvertidamente escaladas ou aumentar a instabilidade. Isto é consistente com a obrigação observada no relatório do GGE da ONU de 2015, qual seja, "cooperar no desenvolvimento e aplicação de medidas para aumentar a estabilidade e a segurança no uso das TICs" [29] Mas, mais uma vez, não se trata apenas de Estados, uma vez que empresas privadas e indivíduos também podem tomar medidas cooperativas

---

27 Assembleia Geral das Nações Unidas, Resolução 73/27, Desenvolvimentos no domínio da informação e telecomunicações no contexto da segurança internacional, A/RES/73/27 (5 de dezembro de 2018), <https://undocs.org/en/A/RES/73/27; e Assembleia Geral das Nações Unidas, Resolução 73/266, https://undocs.org/A/RES/73/266>

28 Relatório 2015 do GGE da ONU, p.7, § 13(a), <https://undocs.org/A/70/174>

29 Id.

para ajudar a garantir a estabilidade do ciberespaço. Por exemplo, as empresas privadas podem trabalhar em conjunto para mitigar ameaças cibernéticas e os indivíduos podem garantir que estão empregando melhores práticas, como atualizações, aplicação de patches, e uso de autenticação multi-fator, para reduzir o risco de que *botnets* assumam o controle das suas máquinas e, em seguida, lançem ataques amplos, que ameaçam a estabilidade do ciberespaço.

D. Princípio dos Direitos Humanos

O quarto princípio reconhece a importância de proteger os Direitos Humanos como um elemento importante da estabilidade do ciberespaço. À medida que a dependência dos indivíduos nas tecnologias da informação e da comunicação aumenta, o efeito disruptivo sobre a atividade humana resultante de ameaças à sua disponibilidade ou integridade é ampliado. Assim, é imperativo que, à medida que os Estados busquem seus interesses estratégicos nacionais no ciberespaço, eles deem a devida atenção aos respectivos impactos sobre os indivíduos, em particular nos seus direitos humanos. De forma semelhante, os atores não estatais devem considerar e minimizar os riscos que as suas atividades representam para o exercício dos direitos on-line e off-line dos indivíduos. No mínimo, o cumprimento do Princípio dos Direitos Humanos exige que os Estados cumpram as suas obrigações em matéria de direitos humanos ao abrigo do direito internacional, ao se envolverem com atividades no ciberespaço.

Os direitos humanos universalmente aceitos estão consagrados na Declaração Universal dos Direitos Humanos. [30] Além disso, um grande número de acordos internacionais que preveem uma variedade de direitos humanos específicos foram adotados e criam obrigações legais vinculativas para os Estados-partes. No contexto do ciberespaço, a aplicabilidade do direito internacional dos direitos humanos foi explicitamente confirmada em várias ocasiões pela

30 Resolução da Assembleia Geral das Nações Unidas 217 A (III), Declaração Universal dos Direitos Humanos (10 de dezembro de 1948), <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

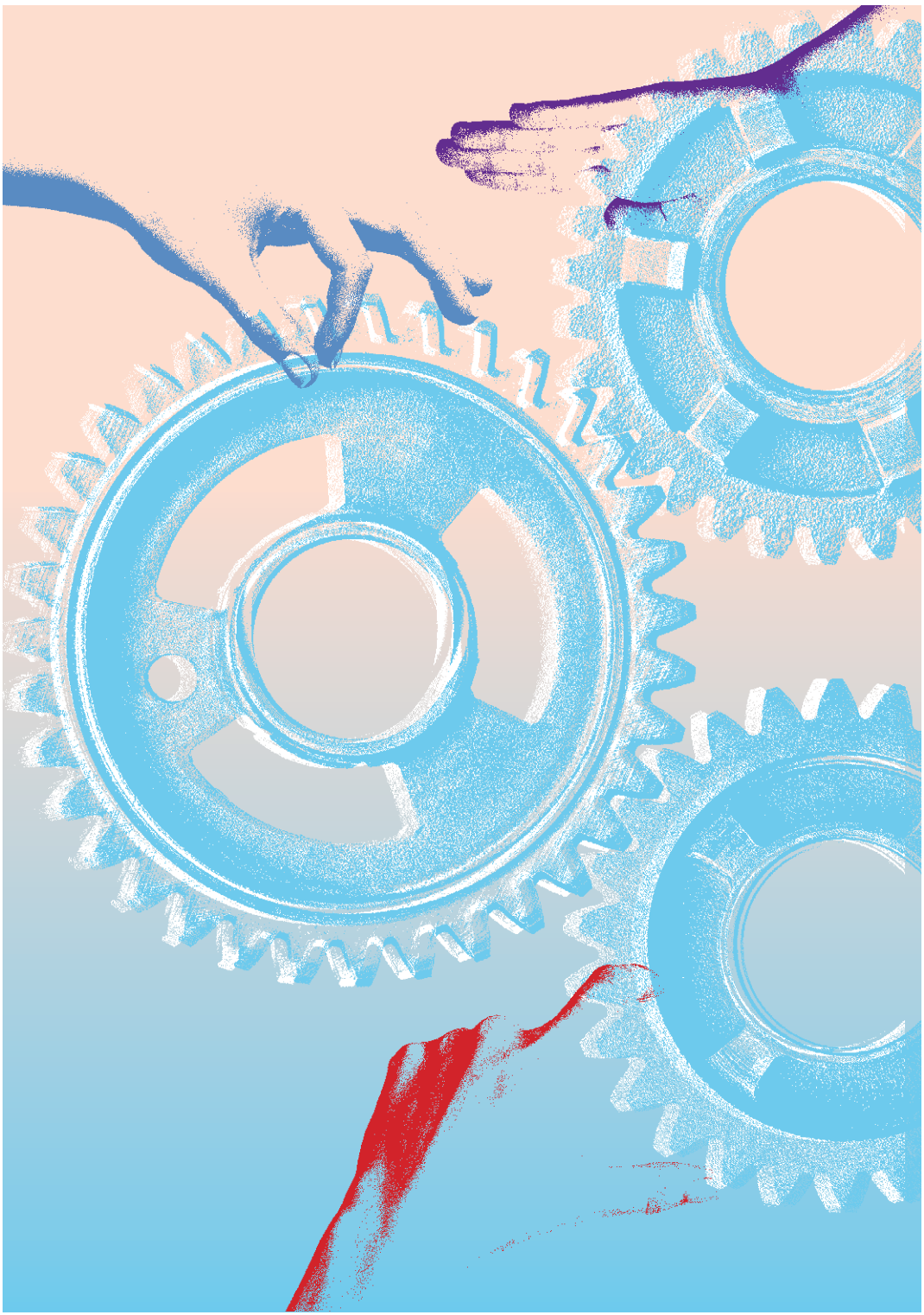
Assembleia Geral das Nações Unidas,[31] pelo Conselho de Direitos Humanos da ONU (HRC, em inglês),[32] bem como pelos relatórios do GGE da ONU de 2013 e 2015.[33] A defesa dos direitos e a garantia aos usuários de que os seus direitos estão sendo respeitados é fundamental para garantir a estabilidade do ciberespaço.

Observamos que os quatro princípios não pretendem ser abrangentes ou cobrir todos os aspectos da política do ciberespaço, e há muitas organizações que produziram amplos conjuntos de princípios que cobrem uma grande variedade de questões. Há também outras organizações focadas em questões relacionadas à governança da Internet e aos direitos humanos on-line (incluindo privacidade, liberdade de expressão e liberdade de associação). Nosso objetivo é alcançar a aceitação generalizada de princípios que apoiam a estabilidade do ciberespaço, especialmente em uma era de atividade hostil sem precedente e sofisticada, onde as regras podem ser pouco claras ou, quando claras, não podem ser adotadas nem aplicadas.

31 Ver Resolução 68/167 da Assembleia Geral das Nações Unidas, O direito à privacidade na era digital, A/RES/68/167 (18 de dezembro de 2013), <https://undocs.org/A/RES/68/167> e Resolução da Assembleia Geral das Nações Unidas 69/166, O direito à privacidade na era digital, A/RES/69/166 (18 de dezembro 2014), <https://undocs.org/en/A/RES/69/166>

32 Conselho de Direitos Humanos das Nações Unidas, A promoção, proteção e exercício dos direitos humanos na Internet, A/ HRC/20/L.13 (29 de junho de 2012), <https://undocs.org/A/HRC/20/L.13>

33 Relatório 2013 do GGE da ONU, https://undocs.org/A/68/98 e Relatório 2015 do GGE da ONU, <https://undocs.org/A/70/174>



VI Normas

Embora os princípios sejam um ponto de partida fundamental para estabelecer políticas e orientar ações táticas, seu alto nível de abstração exige que eles sejam complementados com acordos mais granulares que definam comportamentos aceitáveis. Isto significa que os princípios devem ser complementados por normas. As normas representam comportamentos sociais esperados e apropriados.[34] É impossível discutir normas sem fazer referência ao trabalho de outras organizações, especialmente o GGE da ONU e seu relatório de 2015. [35] O GGE da ONU reconheceu que "tendo em vista os atributos únicos das TIC, normas adicionais poderiam ser desenvolvidas ao longo do tempo"[36] e o mandato da GCSC foi, de fato, "desenvolver propostas de normas e políticas para melhorar a segurança e a estabilidade internacionais." Para desenvolver trabalhos prévios e identificar onde normas adicionais podem ser necessárias, é importante começar com as normas acordadas em 2015, que podem ser encontradas, na sua totalidade, no Apêndice A.

Como o GGE da ONU observou em 2015, ele foi encarregado, entre outras coisas, de "identificar onde pode ser necessário desenvolver normas adicionais que levem em conta a complexidade e os atributos únicos das TICs."[37] Desde então, os produtos e serviços das TIC — bem como o seu mau uso — continuam mudando. Para resolver isso, a GCSC se concentrou em preencher lacunas no atual conjunto de normas, acrescentando especificidade técnica à discussão das normas e abordando questões de implementação. No que diz respeito ao preenchimento de lacunas, por exemplo, a GCSC aprovou uma

34 <https://www.oxfordlearnersdictionaries.com/definition/english/norm_1>
35 Relatório 2015 do GGE da ONU, <https://undocs.org/A/70/174>
36 Id., p.8, § 15.
37 Id., p.7, § 11.

norma para proteger o núcleo público da Internet [38] e uma norma para proteger os sistemas eleitorais. [39] Da mesma forma, enquanto a norma do GGE da ONU se refere à "integridade da cadeia de suprimentos", [40] uma norma da GCSC fala mais especificamente sobre os tipos de ataques da cadeia de suprimentos que devem ser abordados. [41]

A outra grande diferença entre as normas do GGE da ONU e as propostas apresentadas pela GCSC é que a GCSC considera que as responsabilidades devem ser impostas também aos atores não estatais, uma vez que estes devem exercer restrição ou tomar medidas afirmativas para garantir a estabilidade do ciberespaço. Não estamos nos referindo aqui a ataques cibernéticos de criminosos; criminosos que não são dissuadidos pela ação governamental não serão dissuadidos pelas normas. Mas uma vez que a tecnologia muda rapidamente e as leis não, é útil ser preciso sobre quais comportamentos não estatais devem ser encorajados ou desencorajados mesmo na ausência de leis. Por exemplo, alguns defendem que as vítimas de haqueamento devem ter permissão para "haquear de volta" (hack back, em inglês). Mesmo na ausência de leis que permitam ou proíbam tal conduta, a GCSC não a aconselha por várias razões, incluindo o fato de que o invasor inicial pode estar roteando seu ataque através de sistemas

---

38 Comissão Global sobre a Estabilidade do Ciberespaço (GCSC), "Call to Protect the Public Core of the Internet" (New Delhi, Novembro de 2017), <https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf>. Um dos primeiros proponentes da identificação do núcleo público da Internet para proteção especial foi Dennis Broeders, um pesquisador holandês. Ver Dennis Broeders, "The Public Core of the Internet: An International Agenda for Internet Governance" (Amsterdã: Amsterdam University Press, 2015), <https://library.oapen.org/bitstream/handle/20.500.12657/32439/610631.pdf?sequence=1&isAllowed=y>

39 Comissão Global sobre a Estabilidade do Ciberespaço (GCSC), "Call to Protect the Electoral Infrastructure" (Bratislava, maio de 2018), <https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf>.

40 Relatório 2015 do GGE da ONU, p.8, §13(i). Os Estados devem tomar medidas razoáveis para garantir a integridade da cadeia de suprimentos, de modo a que os usuários finais possam ter confiança na segurança dos produtos TIC. "Os Estados devem procurar evitar a proliferação de ferramentas e técnicas maliciosas das TIC e a utilização de funções ocultas nocivas.

41 Comissão Global sobre a Estabilidade do Ciberespaço (GCSC), "Norms Through Singapore" (November 2018), <https://cyberstability.org/wp-content/uploads/2019/04/singaporenew-digital.pdf>. "Os atores estatais e não estatais não devem adulterar produtos e serviços no seu desenvolvimento e produção, nem permitir que sejam adulterados, se isso for prejudicar substancialmente a estabilidade do ciberespaço."

de terceiros (por exemplo, um provedor de nuvem ou um hospital) e, portanto, revidar o haqueamento pode afetar usuários inocentes (por exemplo, clientes de nuvem ou pacientes). Além disso, devido a esses ataques a vítimas inocentes, hackear de volta pode ser visto, ou provocar, um agravamento do problema. Em suma, devido às complexidades levantadas, mesmo na ausência de leis, uma norma que restringe os atores do setor privado pode influenciar o comportamento e, assim, servir um propósito salutar.

A. Normas Propostas pela GCSC

Com os pontos acima em mente, a GCSC desenvolveu as seguintes normas propostas:

1. Os atores estatais e não estatais não devem conduzir nem permitir conscientemente atividades que prejudiquem intencionalmente e substancialmente a disponibilidade geral ou a integridade do núcleo público da Internet e, por conseguinte, a estabilidade do ciberespaço.
2. Os atores estatais e não estatais não devem perseguir, apoiar ou permitir operações cibernéticas destinadas a disrupção da infraestrutura técnica essencial para eleições, referendos ou plebiscitos.
3. Os atores estatais e não estatais não devem adulterar produtos e serviços em desenvolvimento e produção, nem permitir que sejam adulterados, se isso puder prejudicar substancialmente a estabilidade do ciberespaço.
4. Os atores estatais e não estatais não devem apropriar-se dos recursos das TIC do público em geral para sua utilização como *botnets* ou para fins semelhantes.
5. Os Estados devem criar estruturas processuais transparentes para avaliar se e quando devem divulgar vulnerabilidades ou falhas não conhecidas publicamente, e sobre as quais estejam cientes, nos sistemas e tecnologias de informação. A presunção padrão deve ser a favor da divulgação.
6. Os desenvolvedores e produtores de produtos e serviços dos quais depende a estabilidade do ciberespaço devem (1) priorizar a segurança e a estabilidade, (2) tomar medidas razoáveis para garantir que seus produtos ou serviços estejam livres de vulnerabilidades significativas, e (3) tomar medidas para mitigação oportuna das vulnerabilidades que serão posteriormente descobertas e ser transparentes sobre seu processo.

Todos os atores têm o dever de compartilhar informações sobre vulnerabilidades, a fim de ajudar a prevenir ou mitigar atividades cibernéticas maliciosas.

7. Os Estados devem promulgar medidas apropriadas, incluindo leis e regulamentos, para assegurar a higiene cibernética básica.
8. Os atores não estatais não devem participar em operações cibernéticas ofensivas e os atores estatais devem previnir essas atividades e responder caso elas ocorram.

Vale a pena notar que encontrar a linguagem mais apropriada para expressar uma norma pode ser um desafio. Se as normas são demasiado precisas e não deixam margem para interpretação, pode ser difícil chegar a um consenso e pode haver lacunas significativas no seu alcance. Por outro lado, se as normas são muito vagas, elas não fornecem o tipo de orientação necessária para guiar o comportamento e estabelecer expectativas claras para um grupo específico de atores. O objetivo é alcançar o equilíbrio certo e desenvolver novas normas, quando necessário, para garantir que comportamentos indesejados sejam abordados. A título de exemplo, as normas do GGE da ONU adotadas em 2015 protegiam infraestruturas críticas, mas não está claro que o núcleo público da Internet esteja coberto por esse termo; muitos pensam em infraestruturas críticas como utilidades e serviços (por exemplo, energia, comunicações e serviços bancários).[42] Além disso, o GGE da ONU não fez referência especificamente aos sistemas eleitorais,

42 A infraestrutura crítica foi definida como incluindo "sistemas e bens, físicos ou virtuais, tão vitais que a incapacidade ou destruição de tais sistemas e bens teria um impacto debilitante na segurança, segurança econômica nacional, saúde pública ou segurança nacional, ou qualquer combinação desses assuntos". Critical Infrastructures Protection Act de 2001, 42 U.S. Code § 5195c (e), (2001). Também foi definida como "bens ou sistemas vitais para a manutenção das funções sociais, da saúde, da segurança, do bem-estar econômico ou social das pessoas". Conselho da União Europeia, Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção, Jornal Oficial da União Europeia, (8 de dezembro de 2008), <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32008L0114>

uma preocupação que se tornou mais aguda após 2015. [43] Embora os sistemas eleitorais possam ser cobertos em alguns países por referência (isto é, alguns Estados consideram agora os sistemas eleitorais como uma infraestrutura crítica, trazendo-os assim dentro do âmbito das normas de infraestrutura crítica),[44] certos países podem não seguir esta abordagem. Assim, embora o ciberespaço seja global, as proteções normativas podem não ser. Para ajudar a resolver questões de interpretação relativas às normas da GCSC, a Comissão decidiu fornecer um contexto para cada norma acima descrita (ver apêndice B).

Finalmente, as normas de comportamento no ciberespaço não podem ser estáticas. As normas da GCSC refletem um momento no tempo em um cenário tecnológico em constante mudança. Os atores estatais e não estatais devem estar preparados para desenvolver novas normas à medida que as tecnologias avançam e à medida que a nossa compreensão das implicações das tecnologias existentes muda.

Seja com foco nas normas do GGE da ONU, nas normas da GCSC ou em outras normas propostas, deve-se reconhecer que para que as normas sejam eficazes, é necessário que elas sejam adotadas e implementadas, e os infratores das normas devem ser responsabilizados. Abordamos essas questões, antes de nos voltarmos para a forma como os atores não estatais, que são descentralizados e distribuídos ao redor do mundo, podem se unir para trabalhar com os governos em soluções práticas para os desafios da ciberestabilidade.

B. Adoção de Normas

Para que uma norma seja eficaz, ela deve alcançar uma aceitação generalizada. Tal aceitação, mesmo por parte de atores que alguns consideram potenciais violadores de normas, reforça a legitimidade

43 Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks", Fundação Carnegie para a Paz Internacional (23 de maio de 2018), <https://carnegieendowment.org/2018/05/23/russian-election-interference-%20europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435>. Ver também Michael McFaul, ed., Securing American Elections, Stanford Cyber Policy Center (junho de 2019), <https://cyber.fsi.stanford.edu/securing-our-cyber-future>

44 Ver, por exemplo, U.S. Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector" (6 de janeiro de 2017), <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>

de ações que denunciam violações de normas e de ações coletivas apropriadas tomadas para responder a tais violações. Embora a adoção generalizada seja melhor, há espaço para grupos menores de Estados ou de outras entidades que partilham da mesma opinião concordarem e aplicarem normas específicas. Para resolver isso, a GCSC propõe uma abordagem flexível e extensível que permite que os Estados e outras partes interessadas adotem algumas normas enquanto rejeitam ou se abstêm de outras. Esta abordagem não só cria clareza ao destacar áreas específicas de concordância e discordância, como também permite que normas específicas sejam adotadas, aperfeiçoadas e implementadas, mesmo que seja necessário mais tempo para avaliar outras. Em qualquer caso, a adoção generalizada de normas será um esforço de longo prazo.

Há também alguns desafios específicos e práticos para promover a adoção de normas. O desafio específico é o fato de estarmos tentando abordar comportamentos relativamente novos e desestabilizadores. Na medida em que uma norma é "algo usual, típico ou padrão",[45] a elaboração de normas sobre comportamento futuro é um exercício interessante. Se todos já estão se comportando de uma determinada maneira, então uma norma escrita é simplesmente a codificação da prática existente. Mas se não há um "comportamento típico", então a elaboração de uma norma é uma tentativa de encorajar um comportamento comum no futuro, mesmo onde hoje não há um comportamento comum. A simples declaração de que algo é desejável não o tornará normativo, por isso a adoção precisa de ser promovida.

Em segundo lugar, é preciso que haja maior conscientização das normas propostas pelas entidades capazes de implementá-las, bem como aquelas as quais as normas se destinam a proteger. Mesmo com uma atividade significativa na ONU e numa série de outros fóruns, a adoção de normas ainda está em sua relativa infância e muito precisa ser feito para promover normas propostas e garantir sua aceitação, particularmente em certas partes do mundo. É por isso que os esforços de construção de capacitades nesta área são tão vitais; organizações com maior capacidade são mais propensas a apoiar efetivamente a adoção de normas e obter um maior número de adeptos é fundamental para qualquer estrutura normativa global. Além disso, o alcance deve abranger aqueles

45 Ver <https://www.lexico.com/en/definition/norm>

protegidos por normas, pois eles podem não estar cientes de seu potencial impacto. Por exemplo, não parece haver uma consciência generalizada entre as Equipes de Resposta a Emergências Informáticas (CSIRTs/ CERTs) sobre a norma do GGE da ONU relativa aos Estados não atacarem as CSIRTs nacionais e as utilizarem apenas para fins defensivos. Como discutido abaixo, as entidades protegidas muitas vezes terão um papel na implementação e accountability (bem como no desenho da norma proposta), mas não podem cumprir esses papéis se não tiverem consciência ou informação sobre as propostas que estão sendo feitas por atores estatais e não estatais. É claro que os governos e as organizações internacionais precisam fazer mais para alcançar as comunidades que as normas propostas são destinadas a ajudar.

C. Aplicação das Normas

Após a adoção, os atores estatais e não estatais devem tomar medidas concretas para implementar uma norma. Parece haver um crescente consenso nos processos em andamento das Nações Unidas (OEWG e GGE) e nos esforços regionais de que a implementação é uma prioridade. [46] Para alguns, a implementação refere-se à adoção da norma, ao engajamento na construção de capacitades e medidas de construção de confiança, ou à obtenção de um consenso mais granular sobre o significado de uma norma acordada.[47]

---

46 Resolução 73/266 da Assembleia Geral, p. 3, § 1 (b), <https://undocs.org/en/A/RES/73/266>; Resolução 73/27 da Assembleia Geral, p. 5, § 5, <https://undocs.org/en/A/RES/73/27>. Ver também Organização para a Segurança e Cooperação na Europa (OSCE), Discurso de abertura do Secretário-Geral Thomas Greminger, 2019 Presidência da Conferência sobre Segurança Cibernética/ICT a nível da OSCE (Bratislava, 2019). "As organizações regionais...podem ser incubadoras de novas ideias e esforços práticos relacionados com as CBMs, bem como implementadoras de acordos globalmente aceitos, como os relatórios do GGE. Assim, as organizações regionais são incubadoras e implementadoras."

47 A Assembleia Geral da ONU convida todos os Estados Membros, tendo em conta as avaliações e recomendações contidas nos relatórios do GGE e do OEWG, a continuarem a informar o Secretário-Geral sobre os seus pontos de vista e avaliações sobre, nomeadamente, "os esforços envidados a nível nacional para reforçar a segurança da informação e promover a cooperação internacional neste domínio" e "eventuais medidas que possam ser tomadas pela comunidade internacional para reforçar a segurança da informação a nível mundial". Ver relatório 74/120 do Secretário-Geral da ONU, <https://undocs.org/A/74/120>. Para mais pontos de vista nacionais sobre os Estados-Membros, ver <https://www.un.org/disarmament/ict-security/>

Embora estes passos sejam pré-requisitos importantes para a implementação das normas, eles não servem para implementar as próprias normas. Por exemplo, embora a construção de capacidades seja necessária para garantir que os países possam se proteger e ter a largura de banda para se envolver internacionalmente, é possível construir capacidades sem a adoção ou implementação de normas. Do mesmo modo, embora as medidas de construção de confiança possam ajudar a manter a estabilidade do ciberespaço, facilitando o intercâmbio de pontos de vista nacionais sobre a doutrina cibernética, estabelecendo linhas diretas para comunicações rápidas entre especialistas nacionais em matéria de ciberespaço e incentivando o intercâmbio de melhores práticas e práticas de segurança, estas também podem ser feitas sem a implementação de normas. Em vez disso, implementar uma norma envolve a tomada de medidas concretas para lhe dar força. Domesticamente, isto pode incluir a incorporação de normas propostas na política nacional, na legislação e na doutrina militar. Interacionalmente, isto pode incluir a citação de provisões de uma norma quando da atribuição de ataques ou da adoção de medidas diplomáticas. A operacionalização de uma norma desta forma também serve para lhe dar uma definição mais precisa.

D. Accountability

Uma vez adotadas e implementadas as normas, deve haver a accountability daqueles que as violam. Isso levanta questões complicadas de atribuição e resposta, ambas as quais se mostraram desafiadoras na abordagem de ataques cibernéticos.

É necessária uma atribuição crível para embasar uma alegação de que um ator estatal ou não estatal agiu de forma errada. Isso começa com a coleta e análise de provas, e há um trabalho técnico e processual que pode ser feito atualmente para melhorar a qualidade e a cronologia da atribuição. Mais especificamente, como acontece com outras disciplinas técnicas, ter protocolos bem aceitos para coleta e análise de provas é importante para melhorar a qualidade das investigações. Assim, a padronização dos métodos investigativos é importante porque pode reduzir as preocupações sobre a integridade das evidências, mesmo que a atribuição deva ser decidida caso a caso. Além disso, para melhorar a atribuição enquanto uma questão técnica, há muito que pode ser feito para se encurtar os processos burocráticos associados

as decisões sobre atribuição e sua posterior publicização, quando apropriado. O atraso frequente entre um evento e uma declaração de responsabilidade deve-se, em grande parte, a processos pouco claros e difíceis para se chegar a tais decisões a nível nacional, e é agravado quando vários países estão envolvidos na elaboração de declarações de atribuição coletiva. Conceber e exercer processos para determinar a atribuição em nível nacional e internacional, e aprimorar a troca de informações entre países, pode melhorar significativamente a cronologia e a eficácia das declarações de atribuição e facilitar qualquer outra ação apropriada.

Mesmo depois das provas apontarem para um determinado ator, o próximo passo (atribuição) pode continuar sendo um desafio. No passado, alguns atores estatais e não estatais afirmaram que a atribuição seria impossível ou exigiaria prova absoluta. Mas a prova absoluta não é necessária e, embora a atribuição possa ser difícil, não é tão intransponível como alguns sugeriram. No contexto do Estado-nação, a atribuição, seja no domínio cibernético ou físico, é frequentemente um ato político e, embora não exista um padrão de prova particular acordado, os países ainda dispõem de um forte incentivo para não fazer alegações espúrias, a fim de que não percam credibilidade. Em suma, é necessário que a atribuição seja convincente para outros países e para o público.

Mesmo que uma parte lesada esteja convencida de que um determinado ator é responsável (e a atribuição ocorreu de fato em casos internacionais), tornar os atores verdadeiramente imputáveis também demonstrou ser um desafio, prejudicando assim o valor das normas. Afinal, se não houver consequências adversas para aqueles que violam as normas aceitas, essas normas se tornam pouco mais do que palavras no papel e dificilmente desencorajarão atividades desestabilizadoras.

A accountability por ataques cibernéticos conduzidos por atores não estatais é relativamente simples e é predominantemente alcançada através da imposição de responsabilidade civil ou penal ao abrigo das leis nacionais dos Estados em causa. Há certamente desafios ao fazê-lo, uma vez que a natureza internacional de muitos ciberataques e os desafios técnicos na coleta de provas podem constituir obstáculos à ação do Estado. Mas o caminho a seguir é conceitualmente claro: otimizar os processos de aplicação da lei internacional e trabalhar para garantir que criminosos cibernéticos sejam identificados e processados.

Tornar os Estados imputáveis pelas violações das normas é mais desafiador. [48] Isto porque responder a um ataque no ciberespaço dependente fortemente do contexto. Quanto à exigência de accountability, atores estatais e não estatais pesarão fatores diferentes; por exemplo, um Estado que responda a uma violação de normas pode considerar as implicações políticas, enquanto uma empresa do setor privado pode considerar as repercussões comerciais e de reputação. Quanto à forma como uma violação de normas deve ser abordada, as ações estatais disponíveis em resposta a uma violação de normas podem ser vistas ao longo de um continuum, uma vez que uma resposta pode ser menor (por exemplo, uma queixa privada), significativa (por exemplo, sanções econômicas) ou dramática (por exemplo, uma resposta cinética altamente visível). Embora não haja e não haverá uma resposta que sirva para todos os casos, é claro que deve haver consequências significativas para as violações das normas e do direito internacional. Como os esforços anteriores para impor normas tiveram sucesso limitado, são necessárias respostas mais eficazes e oportunas, reconhecendo que tais respostas devem procurar minimizar mais instabilidade.

Os atores não estatais também estão trabalhando para garantir que os violadores das normas sejam responsabilizados por suas ações. Por exemplo, o GFCE [49] combina membros do governo, da sociedade civil e do setor privado para ajudar a coordenar os esforços para construir capacidades, um pré-requisito necessário para a adoção, implementação e accountability das normas. Além disso, o setor privado tem assumido um papel ampliado na atribuição de ataques, utilizando informações proprietárias e públicas para expor os atores e descrever os danos que eles causaram. Finalmente, algumas entidades do setor privado propuseram ou lançaram esforços, como o Instituo de Paz Cibernética (CyberPeace Institute, em inglês)[50]

---

48 Os Estados podem ser responsabilizados pelas operações cibernéticas que realizam, dirigem ou autorizam. O princípio da devida diligência também pode ser útil na definição do nível de cuidado exigido pelos Estados no ciberespaço. Joanna Kulesza, "Due Diligence in International Law", (Leiden: Brill Nijhoff, 2016), <https://brill.com/view/title/26829 >. Ver também , Articles on Responsibility of States for Internationally Wrongful Acts, adotado pela Comissão de Direito Internacional em sua 53ª sessão em 2001, anexado à resolução da Assembleia Geral 56/83 de 12 de dezembro de 2001, e corrigido pelo documento A/56/49(Vol I)/Corr4, artigos 4 e 11, <https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf>

49 Fórum Global de Expertise Cibernética, <https://thegfce.org/>

50 Instituto CyberPeace , <https://cyberpeaceinstitute.org/>

que são projetados para monitorar e expor grandes eventos cibernéticos de forma mais sistemática e potencialmente em maior escala.

Os atores não estatais devem assumir um papel maior em tornar os infratores das normas responsáveis por transgressões. A ideia de aplicação das normas do setor privado não é nova: por exemplo, em 1977, durante a luta antiapartheid na África do Sul, a General Motors promoveu um conjunto de princípios amplamente adotados para fazer negócios (e não fazer negócios) naquele país, resultando em um desinvestimento de mais de 125 empresas estrangeiras. [51] Mais recentemente, e de uma forma mais simbólica, muitas empresas (e governos) responderam ao assassinato saudita do repórter da oposição Jamal Khashoggi boicotando a Iniciativa de Investimento Futuro (Future Investment Iniciative, em inglês) como uma mensagem de desaprovação. [52] Este tipo de esforço é objeto de um exame mais aprofundado.

E. Comunidades de Interesse

Embora uma abordagem multissetorial para adoção, implementação e accountability das normas seja crítica, aproveitar as energias e as capacidades desses grupos é um desafio. Os governos muitas vezes usam o termo "nações com os mesmos ideais" para refletir um grupo de Estados com visões semelhantes, mas não há um termo equivalente que englobe um conjunto de Estados, empresas privadas, organizações sem fins lucrativos (incluindo organizações de normalização), sociedade civil e indivíduos que compartilham opiniões sobre uma questão específica. Isto é importante porque as normas que foram propostas pelo GGE da ONU e pela GCSC podem afetar diferentes constituintes e diferentes organizações e membros da sociedade podem estar interessados em defender certas normas mais do que outras. Como os governos, o setor privado, a comunidade técnica, a academia e a sociedade civil não são entidades monolíticas, é importante pensar em como criar um esforço concertado e não concentrado, que envolva diversas comunidades

51 Ver, em geral, "Sullivan Principles," Wikipedia, 12 de agosto de 2018, <https://en.wikipedia.org/wiki/Sullivan_principles>

52 Ver "Western boycott of Future Investment Initiative 2018," Royal News, 16 de outubro 2018, <https://en.royanews.tv/news/15500/Western-boycott-of-Future-Investment-Initiative-2018>

em questões relacionadas a normas.[53] A criação de Comunidades de Interesse permite que aqueles que têm expertise em normas específicas trabalhem no seu desenvolvimento e implementação. Por exemplo, as Equipes de Resposta a Emergências Informáticas (CERTs/ CSIRTs) podem estar particularmente interessadas em implementar e monitorar a norma do GGE da ONU destinada a proteger essa comunidade, tal como os responsáveis pelos sistemas eleitorais podem estar particularmente interessados na norma da GCSC sobre sistemas eleitorais. Do mesmo modo, a comunidade da Internet poderia ajudar a avançar, implementar e monitorar a norma proposta pela Comissão sobre a proteção do núcleo público da Internet, e os desenvolvedores podem estar mais interessados na norma que envolve a adulteração de produtos.

A formação de uma Comunidade de Interesse pode ser feita mediante um processo dirigido ou ad hoc, de baixo para cima. O fato de os próprios membros poderem formar uma Comunidade não sugere que o seu desenvolvimento e sucesso devam ser deixados ao acaso. Em vez disso, é importante concentrar-se no que faz com que uma Comunidade tenha sucesso: (1) princípios compartilhados; (2) foco na questão; (3) especialização no assunto; (4) apoio financeiro e administrativo; e (5) um processo transparente. Com efeito, pode ser possível identificar um modelo de melhores práticas sobre a forma como as Comunidades devem ser criadas e implementadas, permitindo assim que vários processos de normalização possam alavancar um modelo comunitário semelhante. Isso ajudaria a conciliar diferentes fluxos de trabalho para garantir eficiência e foco, bem como alavancar as práticas recomendadas para adoção, implementação e accountability de normas.

53 Ver, de forma geral, A Era da Interdependência Digital, <https://cgi.br/media/docs/publicacoes/1/20200901150023/CadernoCGIbr_A_era_da_interdependencia_digital.pdf>

VII Recomendações

As nossas seis recomendações para garantir a estabilidade do ciberespaço decorrem dos nossos princípios sobre responsabilidade, restrição, obrigatoriedade de ação e respeito aos Direitos Humanos. Como todos são responsáveis e uma abordagem multissetorial é fundamental para garantir a estabilidade do ciberespaço, nossas recomendações também buscam alavancar as capacidades dos atores estatais e não estatais, em parte através de Comunidades de Interesse. Em suma, nos concentramos no que deve ser feito e na maneira como isso pode ser feito.

1. **Os atores estatais e não estatais devem adotar e implementar normas que aumentem a estabilidade do ciberespaço, promovendo a restrição e incentivando a tomada de ação.** Os atores estatais que anteriormente concordaram com as normas devem definir mais claramente os termos utilizados, um resultado que poderia ser alcançado através de novas negociações e através da experiência prática de aplicação das normas existentes. Tanto os atores estatais quanto os não estatais devem oferecer evidências claras de adoção e implementação de normas através de declarações públicas e de mudanças tanto na política quanto na ação.
2. **Os atores estatais e não estatais, em consonância com suas responsabilidades e limitações, devem responder apropriadamente às violações das normas, garantindo que aqueles que violam as normas enfrentem consequências previsíveis e significativas.** O desenvolvimento e a implementação de normas não serão eficazes se aqueles que violam as normas aprenderem que não há preço para fazê-lo. Por conseguinte, os atores estatais e não estatais devem desenvolver a capacidade interna de avaliar as transgressões e rapidamente decidir e tomar respostas individuais e coletivas adequadas, em consonância com o princípio da obrigatoriedade da ação.
3. **Atores estatais e não estatais, incluindo instituições internacionais, deveriam intensificar os esforços para formar pessoal, desenvolver e construir capacidades, promover entendimento comum da importância da**

estabilidade do ciberespaço e levar em conta as necessidades díspares das diferentes partes . O aumento da capacidade, capacitação e compreensão ampliará a capacidade do mundo para implementar leis, normas e outras medidas de construção de confiança internacionais destinadas a aumentar a estabilidade do ciberespaço, respeitando ao mesmo tempo os Direitos Humanos. Todas as partes devem aproveitar as organizações existentes, incluindo o multissetorial Fórum Global de Expertise Cibernética, que estão focadas na construção de capacidades, já que este é um pré-requisito para adotar e implementar normas, assegurar accountability, tomar outras medidas de estabilidade e respeitar os Direitos Humanos.

4. **Os atores estatais e não estatais deveriam coletar, compartilhar, revisar e publicar informações sobre violações de normas e o impacto de tais atividades.** Embora o mundo tenha visto ações que constituiriam uma violação das normas estabelecidas nas Nações Unidas, e propostas pela GCSC, os relatos tendem a ser anedóticos ao invés de abrangentes. As organizações, particularmente as que são independentes de qualquer interesse estatal ou comercial, devem sistematicamente coletar e publicar informações sobre violações de normas e seu impacto. Isso servirá para catalisar as respostas dos atores estatais e não estatais às violações das normas e servir para melhorar o cumprimento das mesmas.
5. **Os atores estatais e não estatais deveriam estabelecer e apoiar Comunidades de Interesse para ajudar a garantir a estabilidade do ciberespaço.** O estabelecimento e o apoio das Comunidades servirão para garantir que todas as partes interessadas, incluindo os Estados, o setor privado, a comunidade técnica, a academia e a sociedade civil, cumpram com sua responsabilidade de garantir a estabilidade do ciberespaço. Essas Comunidades podem se concentrar, entre outras coisas, na interpretação, adoção e implementação das normas de segurança cibernética apresentadas neste relatório e em outros lugares, se os padrões de evidência para atribuição forem robustos, e se os infratores das normas forem responsabilizados em tempo hábil e de maneira eficaz.
6. **Seja criado um mecanismo de engajamento multissetorial permanente para abordar questões de estabilidade,**

onde os Estados, o setor privado (incluindo a comunidade técnica) e a sociedade civil sejam adequadamente envolvidos e consultados. O Princípio de Responsabilidade reconhece que todos têm um papel a desempenhar na garantia da estabilidade do ciberespaço e reforça a necessidade de abordagens multissetoriais. De 2011 a 2017, a Conferência Global sobre Espaço Cibernético (GCCS, em inglês) proporcionou uma plataforma para tal engajamento que trouxe participantes de nível ministerial dos ministérios das relações exteriores e de segurança que foram encarregados de alcançar estabilidade global em outros contextos, e foi também o ponto de lançamento do Fórum Global de Expertise Cibernética, um importante esforço de construção de capacidades. O Fórum de Governança da Internet (IGF, em inglês) também ofereceu uma plataforma importante para o debate multissetorial. Mais recentemente, o Chamado de Paris (Paris Call, em inglês) reuniu a maior comunidade multissetorial de apoiadores de normas de segurança cibernética. Estes esforços sugerem que é chegado o momento para o desenvolvimento de uma comunidade multissetorial global, inclusiva e orientada para a ação, focada na implementação prática das normas de segurança cibernética apresentadas neste relatório e em outros lugares. O mecanismo deve ser apoiado por uma estrutura permanente para garantir um esforço sustentado e contínuo.

Apêndices

NORMAS ADOTADAS PELO GGE da ONU

a. Os Estados, em consonância com os propósitos das Nações Unidas, incluindo a manutenção da paz e segurança internacionais, devem cooperar no desenvolvimento e aplicação de medidas para aumentar a estabilidade e a segurança no uso das TICs e evitar práticas no domínio das TIC que sejam consideradas prejudiciais ou que possam colocar em risco a paz e a segurança internacionais
b. No caso de incidentes TIC, os Estados devem considerar toda a informação relevante, incluindo o contexto mais amplo em que se produziu o evento, os desafios da atribuição no ambiente de TIC e a natureza e extensão das consequências;
c. Os Estados não devem, conscientemente, permitir que o seu território seja utilizado para atos ilícitos internacionais que utilizem TICs;
d. Os Estados devem ponderar a melhor forma de cooperar para trocar informações, prestar assistência mútua, processar a utilização terrorista e criminosa das TICs e aplicar outras medidas de cooperação para enfrentar essas ameaças. Os Estados podem ter que considerar a necessidade de desenvolver novas medidas a este respeito;
e. Os Estados, para garantir o uso seguro das TICs, devem respeitar as resoluções 20/8 e 26/13 do Conselho de Direitos Humanos sobre a promoção, proteção e exercício 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 pleno respeito aos direitos humanos, incluindo ao direito à liberdade de expressão;
f. Um Estado não deve conduzir ou apoiar conscientemente atividades no domínio das TIC contrárias às obrigações que lhe incumbem em virtude do direito internacional que prejudique intencionalmente as infraestruturas críticas ou prejudique de outro modo a utilização e o funcionamento de infraestruturas críticas para prestar serviços ao público;
g. Os Estados devem tomar medidas apropriadas para proteger a sua infraestrutura crítica de ameaças relacionadas às TIC, tendo em conta a Resolução 58/199 da Assembleia Geral

sobre a criação de uma cultura global de cibersegurança e proteção das infraestruturas críticas de informação, bem como outras resoluções pertinentes;

h. Os Estados devem responder aos pedidos apropriados de assistência apresentados por outro Estado cuja infraestrutura crítica esteja sujeita a atos maliciosos no domínio das TIC. Os Estados devem também responder aos pedidos apropriados para mitigar a atividade maliciosa das TIC que visam à infraestrutura crítica de outro Estado originada em seu território, tendo em conta a devida consideração pela soberania;
i. Os Estados deve tomar medidas razoáveis para garantir a integridade da cadeia de suprimentos, de modo que os usuários finais possam ter confiança na segurança dos produtos de TIC. Os Estados devem procurar evitar a proliferação de ferramentas e técnicas maliciosas no âmbito das TIC e a utilização de funções ocultas nocivas;
j. Os Estados devem incentivar a comunicação responsável das vulnerabilidades das TIC e partilhar informações associadas sobre os recursos disponíveis para essas vulnerabilidades, a fim de limitar e eventualmente eliminar potenciais ameaças às TICs e às infraestruturas dependentes dessas tecnologias;
k. Os Estados não devem realizar ou apoiar conscientemente atividades para prejudicar os sistemas de informação das equipes autorizadas de resposta a emergências (por vezes conhecidas como equipes de resposta a emergências de computador ou grupos de resposta a incidentes de segurança cibernética) de outro Estado. Um Estado não deve usar equipes de resposta de emergência autorizadas para se envolver em atividades internacionais maliciosas.

AS NORMAS DA GCSC

1. Não Interferência com o Núcleo Público

NORMA

Os atores estatais e não estatais não devem conduzir nem permitir conscientemente atividades que prejudiquem intencionalmente e substancialmente a disponibilidade geral ou a integridade do núcleo público da Internet e, por conseguinte, a estabilidade do ciberespaço.

CONTEXTO

Definir o núcleo público da Internet é um desafio, já que muitos tipos diferentes de ataques podem, em última análise, prejudicar a disponibilidade geral ou a integridade da Internet como um todo (resultado a ser evitado). Dito isto, há claramente determinados componentes que seriam visados para que se tenha um impacto dessa amplitude, e é possível ao menos fornecer uma lista não exaustiva de tais elementos críticos. No mais alto nível, a Comissão define a expressão "disponibilidade geral" para significar que o comportamento do ator tem um impacto substancial na população em geral. Portanto, esta norma reconhece que os Estados que apoiam esta norma ainda podem se envolver em atividades que são mais limitadas em propósito e escopo e não têm impacto substancial sobre a população em geral.

A Comissão define a expressão "núcleo público da Internet" de modo a incluir elementos críticos da infraestrutura da Internet, tais como roteamento e encaminhamento de pacotes, sistemas de nomes e números, mecanismos criptográficos de segurança e identidade, mídia de transmissão, software e centros de processamento de dados.

Os elementos de roteamento e encaminhamento de pacotes incluem, mas não são limitados a, (1) equipamentos, instalações, informações, protocolos e sistemas que facilitam a transmissão de comunicações em pacotes de suas fontes para seus destinos; (2) Pontos de Troca de Tráfego (os lugares físicos onde a largura de banda da Internet é produzida); (3) o peering e os roteadores de núcleo das principais redes que transportam essa largura de banda para os usuários; (4) sistemas necessários para garantir a autenticidade do roteamento e defender a rede contra

comportamentos abusivos; (5) design, produção e cadeia de fornecimento de equipamentos usados para os fins acima; e (6) integridade dos próprios protocolos de roteamento e seus processos de desenvolvimento, padronização e manutenção.

Os sistemas de nomes e números incluem, entre outros (1) os sistemas e informações usados na operação do Sistema de Nomes de Domínio da Internet (incluindo registros, servidores de nome, conteúdo de zona, infraestrutura e processos como o DNSSEC, usado para assinar registros criptograficamente); (2) os serviços de informação WHOIS para a zona raiz, hierarquia de endereços inversa, domínios de código de país, geográficos e de nível superior internacionalizados e para novos domínios de nível superior genéricos e não militares; (3) os resolvedores de DNS recursivos públicos frequentemente utilizados; (4) os sistemas da Autoridade para Atribuição de Números de internet e dos Registros Regionais da Internet que disponibilizam e mantêm a alocação única de endereços de Protocolo de Internet, Números de Sistemas Autônomos e Identificadores de Protocolo de Internet; e (5) os próprios protocolos de nomes e números e a integridade dos processos e resultados dapadronização para o desenvolvimento e manutenção de protocolos.

Os mecanismos criptográficos de segurança e identidade incluem, entre outros (1) chaves criptográficas usadas para autenticar usuários e dispositivos e transações seguras na Internet; (2) equipamentos, instalações, informações, protocolos e sistemas que permitem a produção, comunicação, uso e descontinuação dessas chaves; (3) servidores de chaves PGP, Autoridades Certificadoras e sua Infraestrutura de Chaves Públicas; (4) DANE e seus protocolos e infraestrutura de suporte; (5) mecanismos de revogação de certificados e logs de transparência; (6) gestores de senhas; (7) autenticadores de acesso em roaming; (8) mecanismos de tempo preciso e estabelecimento de precedência temporal, como o Protocolo de Tempo para Redes e sua infraestrutura; (9) a integridade dos processos e resultados de padronização para o desenvolvimento e manutenção de algoritmos criptográficos e protocolos; e (10) o design, produção e cadeia de abastecimento de equipamentos usados para implementar processos criptográficos.

As mídias de transmissão incluem, entre outros (1) infraestruturas, sistemas e instalações para comunicações ao serviço do público, seja fibra, cobre ou sem fio; (2) cabos terrestres e

submarinos e estações de aterragem, centros de processamento de dados e outras instalações físicas que os suportem; (3) celulares e outras comunicações de voz e dados sem fios; (4) comunicações de difusão regulamentadas e não regulamentadas; (5) sistemas de suporte para transmissão, regeneração de sinais, ramificação, multiplexação e discriminação sinal-a-ruído; e (6) sistemas de cabo que atendem regiões ou populações, mas não aqueles que atendem clientes de empresas individuais.

Software inclui, mas não está limitado à disponibilidade e integridade dos processos de desenvolvimento, código fonte e infraestrutura de distribuição de patches de software utilizado no núcleo da Internet e por grandes partes do público usuário da Internet.

Os centros de processamento de dados incluem, mas não estão limitado , (1) as instalações físicas que abrigam servidores, conteúdo e a infraestrutura da Internet; (2) o sistema usado para garantir segurança, proteção, controle de acesso físico, operações, gerenciamento, manutenção e sistemas de redundância do centro; e (3) os sistemas de comunicações usados para enviar comunicações para, de, e dentro de centros de processameto de dados.

Os especialistas acreditam que muitas outras categorias de infraestruturas de Internet e de TIC merecem ser protegidas, portanto, esta definição pode ser ampliada no futuro.

2. Proteção das Infraestruturas Eleitorais [54]

NORMA

Os atores estatais e não estatais não devem perseguir, apoiar ou permitir operações cibernéticas destinadas a disrupção da infraestrutura técnica essencial para eleições, referendos ou plebiscitos.

CONTEXTO

De todas as regras, preceitos e princípios que norteiam a conduta dos Estados no princípio de cortesia das nações, a norma da não interferência talvez seja considerada a mais sagrada. O artigo 2(4) da Carta das Nações Unidas articula essa norma e a eleva como um princípio de caráter jurídico e, portanto, vinculativo:

> *Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a independência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas.*

Através desta disposição, os formuladores da Carta reconheceram que as ameaças mais graves ao princípio da não intervenção provêm de medidas coercivas dirigidas à autonomia física ou política de um Estado, pois, de fato, ambas são essenciais para a soberania estatal. O território controlado por um Estado pode ser uma manifestação de sua capacidade soberana, mas é inútil sem o exercício da ação política e independência. Além disso, nada reflete mais a verdadeira independência política do que os processos participativos nacionais, como as eleições, conduzidos de forma livre e justa. A Carta das Nações Unidas procurou conceder fortes proteções contra interferências externas indevidas.

Essas medidas de proteção passaram a ser novamente contestadas na era digital.

Especialistas têm debatido se o tipo de interferência eleitoral cibernética recentemente vista é uma violação ilegal da

---

54 Ver Assembleia Geral das Nações Unidas, Relatório do Grupo de Especialistas Governamentais sobre os Desenvolvimentos na Área de Informação e Telecomunicações no Contexto da Segurança Internacional, A/70/174 (22 de julho de 2015), <https://undocs.org/A/70/174>

soberania (porque interfere no exercício de uma função inerentemente governamental) ou uma intervenção ilegal.[55] Quer tenha ou não ocorrido uma violação do direito internacional, no entanto, existe a clara possibilidade de que atores maliciosos - atuando sozinhos, coletivamente ou em nome dos Estados - manipulem as eleições através de meios digitais. Com os processos participativos nacionais se tornando mais complexos em escala e sofisticação, tem havido uma explosão de dados, instituições e infraestrutura para gerenciá-los. Muitos países publicam hoje as suas listas eleitorais - uma garantia básica e tradicional contra a manipulação ou fraude do voto - online, expondo tais bases de dados a ataques e exploração cibernética. Da mesma forma, os instrumentos de votação eleitoral são utilizados em zonas distantes e remotas de um país, onde os seus operadores não estão totalmente a par dos riscos e das preocupações associadas à sua manipulação digital. Os fornecedores de software de votação e os sistemas informatizados a nível local ou de "cabine" também continuam susceptíveis a tais intrusões.

Ao perceber o crescente número e intensidade de ameaças aos processos participativos, e reconhecendo que tais ataques são inaceitáveis, a GCSC recomenda medidas nacionais mais fortes e cooperação internacional eficaz para prevenir, mitigar e responder às invasões cibernéticas contra a infraestrutura eleitoral técnica. A Comissão reconhece que a condução real de eleições ou processos participativos a nível regional, local ou federal é da competência dos Estados, a ser realizada de acordo com suas respectivas leis nacionais. No entanto, os ataques cibernéticos à sua infraestrutura eleitoral podem ter origem fora de suas fronteiras, o que requer uma resolução de cooperação multilateral. À medida que mais países optam por digitalizar seus mecanismos eleitorais, os riscos e vulnerabilidades associados a essa infraestrutura se multiplicam, assim como a perspectiva de uma ampla, operação cibernética ofensiva. Assim, os governos devem comprometer-se a abster-se de se envolver em operações

55 Ver Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," Chicago Journal of International Law, Vol. 19, No. 1, and Nicholas Tsa- gourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," <https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and--the-principle-of-non-intervention-in-cyberspace/>

cibernéticas contra a infraestrutura técnica eleitoral de outro Estado. Ao recomendar essa norma, a Comissão apenas afirma que a interferência eleitoral é intolerável, quer seja ou não considerada uma violação do direito internacional.

3. Norma para Evitar Adulteração

NORMA

Os atores estatais e não estatais não devem adulterar produtos e serviços em desenvolvimento e produção, nem permitir que sejam adulterados, se isso puder prejudicar substancialmente a estabilidade do ciberespaço.

CONTEXTO

Com uma norma centrada na "Não interferência com o núcleo público da Internet", a GCSC apelou a atores estatais e não estatais para não prejudicar intencional e substancialmente a disponibilidade geral ou integridade do núcleo público da Internet. Em apoio a esta norma, a Comissão registrou a crescente dependência de outras infraestruturas de uma Internet estável e segura e as potenciais consequências dramáticas da sua disrupção. Enquanto a norma de núcleo público se concentrou no "núcleo da Internet", indivíduos e organizações dependem fortemente de certos produtos comerciais para alcançar esse núcleo público e aproveitar a conectividade que ele fornece. Como resultado, adulteração de componentes-chave em produtos de software e hardware de TI (incluindo, mas não limitados a, sistemas operacionais, sistemas de controle industrial, interruptores, roteadores e outros equipamentos críticos de rede, produtos e padrões criptográficos críticos, design de microchips e aplicativos de consumo de usuário final amplamente utilizados) pode igualmente privar a sociedade da capacidade de usar e alavancar a Internet de forma segura e protegida, e enfraquecer globalmente a confiança em seu funcionamento adequado. Embora tais ataques estejam frequentemente nas notícias, o que recebe menos atenção é o fato de um ataque poder ocorrer mesmo antes de um produto ou a sua atualização chegar ao mercado. Por exemplo, um produto pode ser atacado mediante a inserção de uma vulnerabilidade - ou pela remoção secreta de um recurso de segurança - durante a fase de design e fabricação ou durante uma de suas atualizações. Dito de outra forma, um produto pode ser adulterado antes do seu lançamento ou produção, com consequências para o público em

geral. O tempo entre a inserção de uma vulnerabilidade, e a ativação da vulnerabilidade para uso malicioso, pode variar.

Os Estados têm interesses e responsabilidades conflitantes quando lidam com produtos das tecnologias da informação. Por um lado, eles têm a obrigação de promover a resiliência e integridade da infraestrutura cibernética para ajudar a impedir futuros ataques cibernéticos por atores maliciosos e tornar todo o ecossistema digital mais seguro. Por outro lado, os Estados têm a obrigação para com os seus cidadãos de proteger a segurança nacional e combater criminosos e outros atores maliciosos no ciberespaço. A exploração de vulnerabilidades em produtos e serviços digitais utilizados por adversários tem sido alavancada pelos Estados para alcançar sua missão de segurança nacional e proteção pública. Assim, na medida em que os Estados consideram a exploração das vulnerabilidades como uma abordagem eficaz para o cumprimento das suas responsabilidades, podem também considerar útil introduzir intencionalmente fraquezas ou backdoors nos produtos e serviços utilizados pelos adversários. Os atores não estatais podem, por sua vez, também manipular produtos e serviços, uma vez que os seus objetivos podem ser auxiliados pela sua capacidade disruptora da estabilidade do ciberespaço. É importante notar que a norma proíbe a adulteração de um produto ou linha de serviço, que coloca a estabilidade do ciberespaço em risco. Esta norma não proíbe uma ação específica do Estado que apresente pouco risco para a estabilidade geral do ciberespaço; por exemplo, a intercepção e manipulação direcionadas a um número limitado de dispositivos de usuários finais, a fim de facilitar uma espionagem militar ou investigações criminais. Este tipo de atividade, a menos que ocorra dentro da infraestrutura básica do próprio núcleo público, ou enfraqueça criticamente a confiança do usuário na Internet globalmente, é improvável que enfraqueça a confiança geral no ciberespaço, que é uma condição de ciberestabilidade. Embora um ator não estatal possa também visar sistemas de forma limitada, essa atividade pode violar as leis criminais e civis existentes.

Embora os atores estatais e não estatais não devam, afirmativamente, adulterar produtos em desenvolvimento ou produção, os atores do setor industrial também têm a responsabilidade de impedir tais atividades. Portanto, aqueles que criam produtos e serviços devem se comprometer com um nível razoável de

diligência no design, desenvolvimento e entrega de produtos e serviços que priorizem a segurança e, por sua vez, reduzam a probabilidade, frequência, exploração e gravidade das vulnerabilidades. Os envolvidos devem também rejeitar quaisquer esforços aparentes, estatais ou não estatais, para comprometer produtos e serviços, bem como adotar práticas que reduzam o risco de adulteração e lhes permitam responder, caso a adulteração seja detectada.

4. Norma Contra o Comando de Dispositivos TIC em *Botnets*

NORMA:

Os atores estatais e não estatais não devem apropiar-se dos recursos das TIC do público em geral para sua utilização como *botnets* ou fins semelhantes.

CONTEXTO

Os dispositivos conectados à Internet estão se tornando parte integrante da vida das pessoas em todo o mundo. Estamos rodeados de dispositivos com uma multiplicidade de capacidades computacionais, de rede, de detecção e de atuação. Termostatos, televisores, dispositivos médicos, relógios de alarme e automóveis têm capacidade computacional, de armazenamento e de rede que podem ser sequestradas e abusadas. A exploração de vulnerabilidades em seu código subjacente pode levar a problemas de segurança física para os indivíduos que utilizam o dispositivo: um dispositivo que trabalhe fora de seus parâmetros de design pode pegar fogo ou criar outras condições inseguras, como portas inesperadamente destrancadas, transmissão de vídeo a partir do interior de uma casa ou causar falhas em equipamentos (médicos).

Referimo-nos a *botnets* quando os agentes de software são instalados, em massa e sem consentimento, para utilizar os recursos computacionais, de armazenamento ou de rede dos dispositivos. Esses *botnets* podem então ser utilizados para exercer efeitos diretos sobre um sistema alvo diferente, que pode incluir o impacto na confidencialidade, disponibilidade e integridade dos dados dos alvos finais. Portanto, um dispositivo potencialmente não envolvido de "terceiros", e seu proprietário/operador, são parte de uma atividade cibernética maliciosa sem o seu conhecimento. O comprometimento dos dispositivos para instalar agentes de software malicioso não só enfraquece a defesa do dispositivo contra outros ataques — por exemplo, de criminosos — ou infringe o funcionamento normal dos dispositivos, mas também lança o proprietário/operador como potencialmente culpado pelos danos causados ao alvo final. Isto é particularmente evidente nos casos em que o comprometimento do dispositivo pode inadvertidamente lançar o dispositivo e seu proprietário/operador como um beligerante

involuntário em hostilidades interestatais e, portanto, convidar represálias ou responsabilização.

À medida que nos tornamos cada vez mais dependentes da tecnologia em nosso ambiente pessoal, e cada vez mais dispositivos conectados entram no mercado, a exploração de dispositivos de consumo e seu uso como *botnets* compromete cada vez mais a confiança e desestabiliza a sociedade. A Comissão reconhece que existem casos — por exemplo, para efeitos de aplicação da lei — em que os atores estatais autorizados podem considerar necessário instalar agentes de software em dispositivos de um adversário individual específico ou de um grupo de adversários. No entanto, os atores estatais e não estatais não devem comandar dispositivos civis do público em geral (em massa) para facilitar ou executar diretamente operações cibernéticas ofensivas, independentemente da motivação. [56]

56 Esta norma é complementar à norma proposta anteriormente para os atores estatais e não estatais, a fim de evitar a adulteração de produtos antes do seu lançamento, que se concentra nos aspectos da cadeia de abastecimento, enquanto esta norma aborda os dispositivos já implantados.

5. Norma para que os Estados Criem um Processo de Ações Sobre Vulnerabilidades (VEP)

NORMA

Os Estados devem criar estruturas processuais transparentes para avaliar se e quando devem divulgar vulnerabilidades ou falhas não conhecidas publicamente, e sobre as quais estejam cientes, nos sistemas e tecnologias de informação. A presunção padrão deve ser a favor da divulgação.

CONTEXTO

À medida que a complexidade dos sistemas operacionais, softwares critícos, e hardware computacionais cresce, eles passam a conter cada vez mais vulnerabilidades. Essas vulnerabilidades podem ser exploradas por atores estatais e não estatais. Os Estados têm, por vezes, interesses e responsabilidades conflitantes quando lidam com vulnerabilidades recentemente descobertas. Por um lado, têm a obrigação de promover a resiliência e integridade da infraestrutura essencial para a estabilidade do ciberespaço e de tornar todo o ecossistema digital mais seguro para todos os usuários ajudando a impedir a atividade cibernética maliciosa. Isto exigiria que um Estado divulgasse rapidamente vulnerabilidades recentemente descobertas a fornecedores e fabricantes para aplicação de patches, bem como divulgações públicas mais amplas, quando apropriado, para proteger o público. Por outro lado, os Estados têm a obrigação de proteger seus cidadãos de criminosos, de investigar e processar crimes cibernéticos e de se reservarem o direito de impor sanções que atuem como um impedimento específico e geral contra futuras atividades maliciosas. Uma ferramenta essencial para perseguir atores maliciosos, e atores particularmente sofisticados, como os Estados párias, é a exploração de vulnerabilidades na infraestrutura digital da qual dependem. Os Estados, portanto, muitas vezes argumentam que devem preservar pelo menos algumas capacidades selecionadas, incluindo o uso de vulnerabilidades não reveladas, ou então atores maliciosos extremamente capazes não seriam descobertos e verificados.

Embora seja improvável que os Estados revelem voluntariamente todas as vulnerabilidades que descobrem, houve um movimento recente de vários Estados de se afastarem da presunção de que todas as vulnerabilidades não reveladas serão mantidas,

para uma presunção da revelação em favor do interesse de uma maior cibersegurança sistêmica. Uma parte fundamental disso é a criação, pelos Estados, de um processo descrito publicamente para avaliar os prós e os contras da divulgação que leva em conta toda a gama de ações políticas, econômicas, sociais e técnicas. Mais especificamente, esse processo deve ser processualmente transparente e levar em conta uma gama completa de pontos de vista, incluindo fatores como: segurança e resiliência de redes, segurança dos usuários e seus dados, aplicação da lei e utilidade da segurança nacional, e implicações diplomáticas e comerciais. Os Estados Unidos promulgaram recentemente uma nova versão desse processo e outros países estão considerando criar seus próprios processos de ações sobre vulnerabilidades (Vulnerability Equities Process -VEP, em inlês). Dado que a descoberta e a divulgação de vulnerabilidades é mais ampla do que qualquer Estado, a fim de promover a resiliência da rede e, ao mesmo tempo, salvaguardar a segurança nacional, seria no interesse da estabilidade a longo prazo do ciberespaço que cada Estado tivesse um processo desse tipo em vigor. Além disso, os Estados devem trabalhar com vistas a processos compatíveis e previsíveis. A existência de tais processos pode atuar como uma medida de construção de confiança entre os Estados, uma vez que proporcionaria alguma garantia de que as ações relevantes e os interesses concorrentes são plenamente considerados. É claro que cada Estado tem capacidades diferentes e estruturas interinstitucionais únicas; no entanto, qualquer processo de VEP eficaz deve ser projetado levando em conta uma ampla gama de perspectivas e ações. Além disso, embora as decisões tomadas em casos individuais possam, por necessidade, permanecer confidenciais, deve haver transparência quanto aos procedimentos gerais e uma estrutura para se chegar a tais decisões. Finalmente, esta norma trata apenas do estabelecimento de um processo em que as decisões de divulgação são tomadas. Se um governo ou qualquer outra entidade decidir fazer uma divulgação, tal divulgação deve ser feita de forma responsável e que promova a segurança pública e não conduza à exploração dessa vulnerabilidade.

6. Norma para Reduzir e Mitigar Vulnerabilidades Significativas

NORMA

Os desenvolvedores e produtores de produtos e serviços dos quais depende a estabilidade do ciberespaço devem (1) priorizar a segurança e a estabilidade, (2) tomar medidas razoáveis para garantir que seus produtos ou serviços estejam livres de vulnerabilidades significativas e (3) tomar medidas para mitigação oportuna das vulnerabilidades que serão posteriormente descobertas e ser transparente sobre seu processo. Todos os atores têm o dever de compartilhar informações sobre vulnerabilidades, a fim de ajudar a prevenir ou mitigar atividades cibernéticas maliciosas.

CONTEXTO

Certos produtos e serviços de TI são essenciais para a estabilidade do ciberespaço devido à sua utilização dentro da infraestrutura técnica do núcleo, como na resolução ou roteamento de nomes do núcleo, devido à sua ampla facilitação da experiência do usuário da Internet, ou devido à sua utilização dentro de infraestruturas críticas. Aqueles que criam produtos e serviços devem comprometer-se com um nível razoável de diligência no design, desenvolvimento e entrega de produtos e serviços que priorizem a segurança e, por sua vez, reduzam a probabilidade, frequência, exploração e gravidade das vulnerabilidades.

Devido à crescente complexidade de software e hardware, as vulnerabilidades nesses produtos se tornaram fatos. Embora essas vulnerabilidades sejam geralmente não-intencionais , quando descobertas são muitas vezes exploradas, por atores estatais e não estatais maliciosos de modo a minar a estabilidade do ciberespaço.

Além disso, em um mundo hiperconectado e hiperdependente, uma vulnerabilidade descoberta pode afetar vários produtos e serviços através de diferentes produtores e em diferentes ambientes. A aplicação de patches em um produto sem revelar a vulnerabilidade subjacente aos demais pode proteger esse produto, mas não protege a estabilidade do ciberespaço como um todo. Aqueles que estão em melhor posição para avaliar o impacto de uma determinada vulnerabilidade são frequentemente aqueles que desenvolvem, produzem, instalam ou

operam os produtos afetados por vulnerabilidades. É importante compartilhar informações que ajudem a corrigir vulnerabilidades de segurança ou ajudem a prevenir, limitar ou mitigar um ataque. [57]

Embora seja atualmente muito difícil garantir que não existam vulnerabilidades em produtos recém-lançados ou atualizados, a norma proposta, no entanto, sugere que os envolvidos no desenvolvimento ou na produção de tais produtos tomem "medidas razoáveis" que reduziriam a frequência e gravidade das eventuais vulnerabilidades que venham a ocorrer.

Assim como a norma que preconiza a "não adulteração" aborda a inserção intencional de vulnerabilidades em produtos e serviços críticos, e a norma de higiene, em última análise, aborda os deveres dos usuários finais, a norma aqui proposta busca que aqueles que desenvolvem ou produzem produtos críticos tomem medidas razoáveis para garantir que o número e o escopo das vulnerabilidades críticas sejam minimizados e que elas sejam efetivamente e oportunamente mitigadas e, quando apropriado, sejam divulgadas quando descobertas. O processo utilizado deve ser transparente para criar um ambiente previsível e estável.

57 Uma das normas para o comportamento responsável dos Estados no Relatório 2015 do GGE da ONU (A/70/174) afirma que "Os Estados deveriam incentivar a comunicação responsável das vulnerabilidades das TIC e partilhar informações associadas sobre os recursos disponíveis para essas vulnerabilidades, a fim de limitar e eventualmente eliminar potenciais ameaças às TICs e às infraestruturas dependentes dessas tecnologias".

7. Norma Sobre Higiene Cibernética Básica Como Defesa Fundamental

NORMA:

Os Estados devem promulgar medidas apropriadas, incluindo leis e regulamentos, para assegurar a higiene cibernética básica.

CONTEXTO

À medida que a conectividade com a Internet se espalha por todo o mundo, percorrendo todos os aspectos da vida moderna, os usuários de todos os tipos — indivíduos, organizações, empresas e governos — estão cada vez mais dependentes da tecnologia e do acesso às informações disponíveis na Internet. Política, economia, informação pública, educação, desenvolvimento e todas as outras formas de interação social dependem criticamente da Internet e das tecnologias a ela associadas. No entanto, esta maravilha moderna permanece amplamente insegura, e ninguém é imune aos seus perigos.

Ainda não surgiu consenso sobre as formas mais eficazes de otimizar as tecnologias promissoras do ciberespaço, ao mesmo tempo em que se salvaguarde o público. No entanto, a maioria concorda que os benefícios de termos nossas vidas conectadas digitalmente não podem ser sustentados no futuro sem padrões de segurança acordados, que são essenciais no ciberespaço. Para tanto, a Comissão apoia firmemente a adoção generalizada e a aplicação verificada da ciberhigiene básica — um regime de medidas fundamentais que representam tarefas prioritárias e essenciais que devem ser desempenhadas para defender, prevenir e mitigar rapidamente os perigos evitáveis no ciberespaço.

De fato, tendo em vista a abrangência da interconectividade on-line, estas medidas constituem um dever básico de cuidados que deve ser exigido de todos os usuários. Os regimes de higiene devem incorporar medidas de implementação confiáveis, fornecer uma troca generalizada de informações técnicas e de boas práticas e estar sujeitas a uma supervisão adequada. Dispositivos e processos cada vez mais inteligentes exigem leis e regulamentos inteligentes. Ao criar mais accountability por este dever básico de cuidados cibernéticos, os governos não devem restringir a inovação ou alterar as propriedades básicas da Internet.

Os padrões de higiene cibernética já existem de várias formas.[58] Esses padrões têm aceitação internacional cada vez mais ampla, à medida que governos e empresas compreendem cada vez mais a importância de tomar medidas para ajudar a prevenir e reduzir rapidamente os perigos de malwares conhecidos. Além disso, estas normas representam as melhores práticas, destacam a importância de uma supervisão sensata e regular e sublinham a importância do compartilhamento automatizado de informações quando possível para alertar outros usuários sobre problemas. Tais defesas cibernéticas básicas, conforme delineadas nessas abordagens, explicam a realidade de que nenhum governo, organização ou coleção de usuários pode, por si só, aliviar todos os riscos cibernéticos. Elas também reconhecem que os usuários em todos os níveis têm papéis importantes a desempenhar no fortalecimento da segurança cibernética.

A GCSC acredita que a defesa fundamental da segurança cibernética através da adoção generalizada da ciberhigiene tornou-se essencial para o uso responsável e o crescimento benéfico da Internet. A segurança deve ser vista como um processo contínuo, com responsabilidades distribuídas entre todos os atores através dos mecanismos em vigor, tais como relatórios automatizados e compartilhamento de informações, para garantir uma accountability adequada.

A Comissão reconhece igualmente que muitas sociedades em todo o mundo enfrentam desafios consideráveis na utilização das tecnologias da informação e das comunicações e apela aos Estados para que partilhem conhecimentos e ofereçam a construção de capacidades para instanciar processos de aplicação eficaz de regimes básicos de ciberhigiene para expandir o efeito desta norma.

58 Isso inclui, por exemplo, o Instituto Europeu de Normas de Telecomunicações (ETSI), o Centro para Segurança da Internet (CIS), organização sem fins lucrativos, e o Australian Signals Directorate (ASD), entre outros.

8. Norma Contra Operações Cibernéticas Ofensivas Perpetradas por Atores não Estatais

NORMA:

Os atores não estatais não devem participar de operações cibernéticas ofensivas e os atores estatais devem previnir essas atividades e responder caso elas ocorram.

CONTEXTO

Embora as tecnologias da informação e da comunicação tenham transformado positivamente as sociedades, elas também trazem novos desafios de segurança. A rapidez e a onipresença das operações cibernéticas colocam muitas vezes dificuldades consideráveis aos sistemas judiciais dos Estados e à cooperação internacional em matéria de aplicação da lei. Apesar destas dificuldades, importa recordar que a soberania estatal é a pedra angular do sistema internacional de paz e segurança, o qual se baseia em regras. Os Estados têm o monopólio do uso legítimo da força, estritamente vinculados pelo direito internacional. Alguns atores não estatais, principalmente empresas privadas, defendem o direito de realizar operações cibernéticas ofensivas através das fronteiras nacionais, alegando potencialmente que elas constituem uma ação defensiva necessária, uma vez que os Estados não têm capacidade para protegê-los adequadamente contra ameaças cibernéticas. As operações cibernéticas ofensivas desses atores não estatais são às vezes eufemisticamente referidas como "defesa cibernética ativa"[59], incluindo, entre outros o revide de haqueamento ("hack back"), pois são conduzidas para fins defensivos.

Alguns Estados não controlam ou podem ignorar ativamente essas práticas, apesar do risco que impõem à estabilidade e segurança do ciberespaço. No entanto, em muitos Estados tais práticas seriam ilegais, se não criminalizadas, enquanto em outros Estados elas parecem não ser proibidas nem

59 A defesa cibernética ativa deve ser considerada como um conjunto de medidas que vão desde autodefesa na rede da vítima até atividade destrutiva na rede do invasor. As operações cibernéticas ofensivas dentro deste continuum implicam que o defensor atue fora de sua própria rede independentemente da sua intenção (ofensa ou defesa) e da qualificação legal dos seus atos. Deve-se continuar a trabalhar na definição de operações cibernéticas ofensivas e na defesa cibernética ativa.

explicitamente autorizadas. Alguns Estados estão, no entanto, considerando legitimar as operações cibernéticas ofensivas de atores não estatais. Com efeito, alguns decidiram ou propuseram legislação doméstica para permitir operações ofensivas por parte de atores não estatais.

A GCSC acredita que essas práticas minam a estabilidade do ciberespaço. Elas podem resultar em sérias disrupções e danos, inclusive para terceiros, e são, portanto, suscetíveis de desencadear disputas jurídicas complexas e de escalonar conflitos. Os Estados que concedessem explicitamente ou autorizassem conscientemente atores não estatais a realizar operações ofensivas, para os seus próprios fins ou para os de terceiros, criariam um precedente perigoso e correriam o risco de violar o direito internacional. A Comissão acredita que as medidas ofensivas devem ser reservadas exclusivamente aos Estados e recorda que o direito internacional estabelece um quadro rigoroso e exclusivo para a resposta dos Estados a atos hostis que também se aplica às operações cibernéticas. Do mesmo modo, nos termos do direito internacional, os agentes não estatais que atuam em nome dos Estados devem ser considerados seus agentes e, portanto, considerados extensões do Estado. [60]

Se os Estados permitirem tal ação, poderão, por conseguinte, ser responsabilizados nos termos do direito internacional. [61] Estados devem agir, em nível nacional e internacional, para prevenir operações cibernéticas ofensivas por parte de atores não estatais.

---

60 Veja "nota adicional" para um tratamento mais amplo do caso dentro do direito internacional, disponível aqui: <https://cyberstability.org/wp-content/uploads/2018/11/Additional-Note-to-the-Norm-Against-Offensive-Cyber-Operations-by-Non-state-Actors-Norm-Package-Singapore.pdf>

61 Id.

HISTÓRIA, OBJETIVOS E PROCESSOS DA GCSC

Desde o seu lançamento na Conferência de Segurança de Munique, em fevereiro de 2017, sob o patrocínio do ministro de Relações Exteriores dos Países Baixos, Bert Koenders, a Comissão Global sobre a Estabilidade do Ciberespaço tem sido considerada uma das primeiras iniciativas multissetoriais de seu tipo a concentrar-se especificamente na estabilidade do ciberespaço. Presidida por Michael Chertoff, ex-Secretário de Segurança Interna dos Estados Unidos; Latha Reddy, ex-Vice Assessora de Segurança Nacional da Índia; e anteriormente por Marina Kaljurand, Deputada do Parlamento Europeu e ex-Ministra das Relações Exteriores da Estônia, a Comissão é composta por 28 indivíduos proeminentes de diferentes origens e históricos, envolvidos com a cibersegurança internacional.[62] A Comissão é apoiada por Conselheiros Especiais, um Secretariado, sendo composta pelo Centro de Estudos Estratégicos de Haia e pelo Instituto EastWest, um Grupo Consultivo de Pesquisa, além de vários parceiros e patrocinadores, incluindo o Ministério das Relações Exteriores dos Países Baixos e da França, a Agência de Segurança Cibernética de Singapura, a Microsoft, a Internet Society e a Afilias.

A Comissão nasceu do desejo de dar continuidade ao trabalho das comissões anteriores da sociedade civil, incluindo a Comissão Global de Governança da Internet, e de se conectar com o trabalho da Conferência Global sobre o Ciberespaço (GCCS, na sigla em inglês). Em 2015, o Centro de Estudos Estratégicos de Haia (HCSS, na sigla em inglês) foi convidado a organizar uma sessão preparatória para a reunião de Haia da GCCS, dedicada à paz e à segurança internacional. Grande parte da declaração subsequente da GCCS baseou-se diretamente no trabalho da reunião preparatória, traçando claramente a necessidade de um formato multissetorial para discutir questões internacionais de cibersegurança. Assim, o HCSS reuniu um grupo central de apoiadores e financiadores (originalmente a Microsoft, a Internet Society e o Ministério das Relações Exteriores dos Países Baixos) e desenvolveu um plano estratégico. Em agosto de 2016, após conquistar o EastWest Institute (EWI) como parceiro no Secretariado, o HCSS convocou uma reunião do Grupo de Iniciação da GCSC na Harvard Kennedy School, que elaborou os principais requisitos para o funcionamento da GCSC, seus membros, estrutura e objetivos, bem como sua missão.

62 Ver lista completa dos Comissários na página 14.

A declaração da missão diz:

> *A Comissão Global sobre a Estabilidade do Ciberespaço (GCSC) desenvolverá propostas de normas e políticas para melhorar a segurança e a estabilidade internacionais e orientar o comportamento estatal e não estatal responsável no ciberespaço. A GCSC envolverá toda a gama de partes interessadas para desenvolver entendimentos compartilhados e o seu trabalho promoverá a ciberestabilidade, apoiando a pesquisa, o intercâmbio de informações e ao construção de capacidades.*

Desde o início das suas atividades, a GCSC pretendia influenciar a agenda internacional de paz e segurança relacionada ao ciberespaço, geralmente referida como "cibersegurança internacional." O Grupo de Iniciação identificou a necessidade de solicitar visões diversas, especialmente por parte da governança da Internet e das comunidades técnicas, para as discussões internacionais em curso sobre segurança cibernética. O objetivo era informar melhor as deliberações nas comunidades de controle de armas e paz e segurança, onde grande parte do bom trabalho, particularmente em normas, foi considerado dificultado pela falta de contribuição e aceitação por parte desses atores da sociedade civil e do setor privado. Por conseguinte, a abordagem multissetorial foi considerada uma questão prática e não ideológica.

A GCSC abordou suas deliberações de forma "de baixo para cima para de cima para baixo". Em primeiro lugar, ela identificou normas operacionais que atendam as mais óbvias necessidades urgentes de cibersegurança internacional expressas pelos seus membros e que não foram abordadas em nenhum outro lugar. Em segundo lugar, ela extrapolou a partir destas e de normas já existentes uma definição funcional de ciberestabilidade e seus princípios subjacentes. Em terceiro lugar, foi desenvolvida uma estrutura de estabilidade para se obter uma compreensão mais clara do que a arquitetura internacional de paz e segurança precisa fazer para responder a essa definição. Por último, elaborou recomendações dirigidas a partes interessadas estatais e não estatais sobre como isso poderia ser alcançado.

As deliberações dos Comissários em relação a estes objetivos foram conduzidas transversalmente às fronteiras geográficas e os grupos de partes interessadas. Desde o início, a Comissão colocou ênfase na realização das suas reuniões à margem de conferências

relevantes para facilitar a contribuição de uma vasta gama de interessados.[63] Também solicitou ativamente a contribuição através da pesquisas à comunidade em geral. Para conectar o trabalho do GCSC à comunidade acadêmica mais ampla, o Grupo Consultivo de Pesquisa foi instaurado com um presidente e quatro vice-presidentes[64] responsáveis pela gestão de uma lista de e-mails com mais de 200 especialistas. Foi também a base para um amplo programa de pesquisa, que eventualmente encomendou mais de 20 estudos a instituições de pesquisa e indivíduos em todo o mundo.[65] A maior parte deste trabalho foi apresentada diretamente aos Comissários durante as "Audiências sobre Ciberestabilidade".

Antes da publicação deste Relatório e das normas anteriormente publicadas, a Comissão procurou consistentemente a contribuição de um vasto leque de interessados governamentais, da sociedade civil e do setor industrial. Ao escalonar a entrega ao longo de todo o mandato da Comissão, foi possível solicitar constantemente a opinião e comentários externos. Foram emitidos pedidos de consulta on-line sobre as normas da GCSC e a definição de ciberestabilidade. Foram recebidas mais de 23 propostas de atores de todo o mundo, com o intuito de informar as deliberações dos Comissários. Além disso, a Comissão participou ativamente em mais de 70 conferências e eventos e convocou mesas redondas, eventos paralelos e audiências dedicadas à Ciberestabilidade com uma ampla gama de partes interessadas estatais e não estatais.

Por último, os próprios Comissários mantiveram eles mesmos laços ativos com as respectivas comunidades. As contribuições e o feedback destes grupos representaram a base das interações com a comunidade mais ampla de especialistas estatais e não estatais e constituirão a base da defesa do relatório daqui para frente.

---

63 As reuniões oficiais da Comissão foram convocadas para os seguintes eventos: Conferência de Segurança de Munique 2017 (Munique, Alemanha); CyCon (Tallinn, Estônia); BlackHat EUA (Las Vegas, EUA); Conferência Global sobre Ciberespaço (Nova Deli, Índia); Fórum Internacional de Segurança Cibernética 2018 (Lille, França); Conferência de Segurança de Munique 2018 (Munique, Alemanha - Conferral); GLOBSEC (Bratislava, Eslováquia); Semana Cibernética de Israel (Tel Aviv, Israel - Conferral); Semana Internacional Cibernética de Singapura (Singapura); Fórum da Paz de Paris e IGF (Paris, França - Conferral); Instituto das Nações Unidas para a Investigação sobre Desarmamento 2019 (Genebra, Suíça); Fórum Comunitário da ICANN 64 (Kobe, Japão); EuroDIG (Haia, Países Baixos); Reunião Anual do GFCE (Adis Abeba, Etiópia).

64 Abrangendo quatro áreas temáticas, incluindo paz e segurança internacional, direito internacional, governança da Internet e tecnologia.

65 Ver seção de Agradecimentos.

Agradecimentos

A Comissão Global sobre a Estabilidade do Ciberespaço (GCSC) gostaria de agradecer às muitas instituições e aos indivíduos que apoiaram, contribuíram e facilitaram o trabalho da Comissão, incluindo, entre outros, nossos patrocinadores, o Grupo Consultivo de Pesquisa, os autores de trabalhos de pesquisa, os seus pares revisores e equipe de apoio. Abaixo listamos apenas algumas das pessoas que contribuíram para o sucesso da Comissão.

Secretariado

CENTRO DE ESTUDOS ESTRATÉGICOS DE HAIA (HCSS)

Alexander Klimburg
Diretor da Iniciativa e Secretariado da Comissão Global sobre a Estabilidade do Ciberespaço

Louk Faesen
Gerente de Projetos, Secretariado da Comissão Global sobre a Estabilidade do Ciberespaço

Elliot Mayhew
Assistente de Projeto, Secretariado da Comissão Global sobre a Estabilidade do Ciberespaço

Com o apoio adicional de: **Timon Domela Nieuwenhuis Nyegaard, Koen van den Dool, Niels Renssen, e Kaja Karlson**.

INSTITUTO EASTWEST (EWI)

Bruce W. McConnell
Co-Diretor, Secretariado da Comissão Global sobre a Estabilidade do Ciberespaço

Anneleen Rogeman
Gerente de Projetos, Secretariado da Comissão Global sobre a Estabilidade do Ciberespaço

Com o apoio adicional de: **Abagail Lawson, Dragan Stojanovski e Conrad Jarzebowski**

Parceiros, Patrocinadores e Apoiadores

Centro de Estudos Estratégicos de Haia, o Instituto EastWest e os Comissários gostariam de reconhecer e agradecer o apoio das seguintes organizações:

PARCEIROS:

Ministério de Relações Exteriores dos Países Baixos
Timo Koster e Dimitri Vogelaar

Microsoft
Jan Neutze e Kaja Ciglic

Agência de Segurança Cibernética de Singapura
David Koh e Sithuraj Ponraj

Internet Society (ISOC)

Ministério das Relações Exteriores da França
Henry Verdier e David Martinon

Afilias
Ram Mohan e Philipp Grabensee

PATROCINADORES:

Departamento Federal de Relações Exteriores da Suíça

GLOBSEC

Ministério das Relações Exteriores da Estônia

Ministério de Assuntos Internos e Comunicações do Japão

APOIADORES:

Comissão da União Africana

Black Hat EUA

DEF CON

Delegação da União Europeia junto às Nações Unidas em Genebra

Fórum Global de Expertise Cibernética

Google

Prefeitura de Haia

Packet Clearing House

Universidade de Tel Aviv

Instituto das Nações Unidas para a Investigação sobre o Desarmamento

Essas organizações e instituições estão empenhadas em promover o debate e apresentar soluções criativas para alguns dos desafios mais urgentes enfrentados pela estabilidade do ciberespaço.

Pesquisadores

A Comissão gostaria de agradecer aos membros do seu Grupo Consultivo de Pesquisa, um grupo de mais de 200 membros on-line que conectou a GCSC à comunidade acadêmica mais ampla. Em especial, gostaríamos de agradecer aos pesquisadores que foram incumbidos de escrever relatórios e memorandos para informar as deliberações dos Comissários.

RESUMO DA EDIÇÃO 1 DA GCSC (Novembro de 2017)

Alex Grigsby
Ex-membro do Conselho de Relações Exteriores (CFR)

Deborah Housen-Couriel
Konfidas Digital Ltd.

Joanna Kulesza
Universidade de Lodz

Rolf H. Weber
Universidade de Zurique

Oluwafemi Osho
Joseph A. Ojeniyi
Shafi'i M. Abdulhamid
Universidade Federal de Tecnologia, Minna

Analía Aspis
Universidade de Buenos Aires

Robert Morgus
Anteriormente da Nova América

Max Smeets
Anteriormente do Centro de Segurança Internacional e Cooperação, Universidade de Stanford

Trey Herr
Escola Harvard Kennedy

Arun Mohan Sukumar
Madhulika Srikumar
Bedavyasa Mohanty
Fundação Observer Research (ORF)

RESUMO DA EDIÇÃO 2 DA GCSC (Maio de 2018)

Shen Yi
Jiang Tianjiao
Wang Lei
Centro de Pesquisa para a Governança do Ciberespaço, Universidade de Fudan

Elana Broitman
Mailyn Fidler
Robert Morgus
Anteriormente da Nova América

Elonnai Hickok
Arindrajit Basu
Centro para Internet e Sociedade

Thomas Uren
Bart Hogeveen
Fergus Hanson
Instituto Australiano de Políticas Estratégicas (ASPI)

Dragan Mladenović
Vladimir Radunović
Diplofoundation

Thomas Reinhold
Instituto para Pesquisa sobre Paz e Política de Segurança, Universidade de Hamburgo

Consultas

A Comissão gostaria de agradecer às seguintes pessoas e organizações pelo envio de comentários abrangentes em resposta ao Pedido de Consultas sobre o Pacote de Normas de Singapura (de 17 de dezembro de 2018 a 17 de janeiro de 2019) e sobre a Definição de Estabilidade do Ciberespaço (de 14 de agosto de 2019 a 6 de setembro de 2019):

Hussein Abul-Enein
Parceria Access

Kayode Akanni
DesignIT

Jonathan D. Aronson
Universidade do Sul da Califórnia (USC)

Avidiram Atzaba
Direção Nacional Cibernética de Israel

Arindrajit Basu
Gurshabad Grover
Elonnai Hickok
Karan Saini
Centro para Internet & Sociedade

Vytautas Butrimas
Centro de Excelência da Segurança Energética da OTAN

Acordo de Tecnologia de Cibersegurança

Michael Daniel
Aliança Ameaça Cibernética (CTA)

Parceiros Digitais Globais

Arvind Gupta
Dickey Kumar
Fundação Internacional Vivekananda

Tara Hairston
Anastasiya Kazakova
Kaspersky

Sven Herpig
Fundação Nova Responsabilidade (SNV)

Drew Mitnick
Access Now

George M. Moore
James Martin
Centro para estudos de Não-Proliferação

Brett van Niekerk
Trishana Ramluckan
Universidade de KwaZulu-Natal

Peter Swire
Justin Hemmingse Sreenidhi Srinivasan,
Faculdade de Negócios Georgia Tech Scheller

Johan de Wit
Siemens/Universidade Técnica de Delft (TU Delft)

Finalmente, a Comissão gostaria de agradecer aos seguintes especialistas, cujos trabalhos e conhecimentos orientaram e informaram as deliberações da Comissão:

Dennis Broeders
Universidade de Leiden

Deborah Brown
Verónica Ferrari
Associação para Comunicações Progressivas

Michael Daniel
Aliança Ameaça Cibernética (CTA)

François Delerue
Instituto de Pesquisa Estratégica da Escola Militar — IRSEM

Akhil Deo
Arun Mohan Sukumar
Fundação Observer Research (ORF)

Martha Finnemore
Universidade George Washington

Aude Géry
Universidade de Rouen

Duncan Hollis
Escola Temple Law

Joanna Kulesza
Universidade de Lodz

Peter Rowland
Packet Clearing House

Michael Schmitt
Escola de Direito de Exeter

SECRETARIADO

Centro de Estudos Estratégicos de Haia (HCSS)
Intituto EastWest (EWI)

PARCEIROS

Governo dos Países Baixos
Corporação Microsoft
Agência de Segurança Cibernética de Singapura
Ministério das Relações Exteriores da França
Internet Society (ISOC)
Afilias

PATROCINADORES

Departamento Federal de Relações Exteriores da Suíça
GLOBSEC
Ministério das Relações Exteriores da Estônia
Ministério de Assuntos Internos e Comunicações do Japão

APOIADORES

Comissão da União Africana
Black Hat EUA
DEF CON
Delegação da União Europeia junto às Nações Unidas em Genebra
Fórum Global de Expertise Cibernética
Google
Prefeitura de Haia
Packet Clearing House
Universidade de Tel Aviv
Instituto das Nações Unidas para a Investigação sobre Desarmamento

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR