Lívia CARDOSO VIANA GONÇALVES[1]

Resumo:

Esse artigo visa suscitar questões centrais na abordagem das ameaças existentes e potenciais no espaço cibernético utilizando-se análise comparativa entre ordenamentos distintos, bem como da análise de um caso concreto de grande repercussão sistêmica no contexto das infraestruturas críticas. Para tanto, análises relativas a conceitos, políticas, estratégias são objetos de reflexão para concepção de um marco legal ideal/geral com potencialidade de gerenciar melhor a complexidade das ameaças existentes nesse espaço, bem como de promover maior efetividade na implementação da segurança cibernética no âmbitos nacionais e internacionais.

Abstract:

This article aims to raise central questions regarding the approach to existing and potential threats in cyberspace using a comparative analysis between distinct systems, as well as the analysis of a concrete case of great systemic repercussion in the context of critical infrastructures. For this purpose, analyses related to concepts, policies, strategies are objects of reflection for the conception of an ideal / general legal framework with the potential to better manage the complexity of the threats existing in this space, as well as to promote greater effectiveness in the implementation of cyber security within the national and international scope.

Palavras chave: Segurança Cibernética, Estratégias e Marco legal, Infraestrutura crítica
Keywords: *Cyber Security, Strategies and legal framework, Critical Infrastructure*

1 Lívia Cardoso Viana Gonçalves é Graduada e pós-graduada em Direito Público pela Universidade de Brasília, e Mestre em Defesa e Segurança Hemisférica pelo CID. Procuradora Federal de carreira, trabalha desde 2009 no Ministério da Defesa, onde atuou como Consultora Jurídica, Chefe de Gabinete do Ministro da Defesa e Assessora do Ministro em Washington. Condecorações: Medalha Mérito da Defesa, Gran Cruz; Mérito Aeronáutico, Grande Oficial; Mérito Naval, Grande Oficial e Mérito Militar, grau Comendador.

Introdução

A presença militar brasileira no Haiti, por 13 anos, pode, indubitavelmente, ser considerada uma epopeia muito bem sucedida, que correspondeu em sua plenitude aos objetivos visualizados por seus

O advento da globalização trouxe uma grande modificação na forma com que os indivíduos e as empresas se relacionam, bem como alterou o modo de atuação dos Estados, tanto em suas relações no âmbito interno, como nas relações com outros Estados, sendo possível notar uma crescente interdependência. Neste ponto, refiro-me tanto aos processos pelos quais essas relações se perfectibilizam, quanto à sua própria natureza e perspectivas dessas relações. Esse movimento se deve, em grande parte, ao surgimento da internet e de tecnologias relacionadas, bem como seu desenvolvimento no espaço cibernético, como um novo e complexo sistema em contínua modificação.

Neste contexto, este artigo tem por objetivo conhecer melhor o espaço cibernético, as debilidades e ameaças a ele relacionadas, bem como analisar como os diferentes atores tem atuado neste meio para otimizar suas fortalezas e oportunidades. Essa reflexão será realizada à luz dos conhecimentos especificamente relacionados à segurança cibernética,[2] e poderão auxiliar no processo de compreensão, elaboração e execução de políticas conforme uma perspectiva mais holística, integral e flexível, visando maior eficiência.

I. Usuais enfoques e paradigmas contra as ameaças cibernéticas

No cenário atual, extremamente globalizado, vemos a ampliação das oportunidades, bem como dos desafios em igual ou ainda maior grandeza, considerando as características do espaço cibernético[3] e necessidade de promover maior segurança cibernética.[4]

[2] Modulo de Cybersecurity lecionado pelo Kevin P. Newmeyer no Colégio Interamericano de Defesa no curso de ano 2018.

[3] "Por tanto, podemos definir el ciberespacio como el conjunto de medios y procedimientos basados en las TIC y configurados para la prestación de servicios. La definición permite comprender de inmediato que el ciberespacio es ya parte esencial de nuestras sociedades, economías e, incluso, puede

Isso ocorre porque, como apontado por Diniz, "The existence of cyberspace is already generating a massive evolution – indeed a revolution – in all aspects of social, economic and political life".[5] Em outras palavras, pode-se dizer que a composição entre o binômio Desenvolvimento X Defesa tem se tornado cada vez mais complexa.[6] Não

llegar a ser factor determinante de la evolución de las culturas, o quizás de su convergencia. De ahí la importancia de proteger el ciberespacio. Anteriormente, la ciberseguridad obedecía a un enfoque de protección de la información (Information Security) donde solamente se trataba de proteger la información a accesos, usos, revelaciones, interrupciones, modificaciones o destrucciones no permitidas. En la actualidad, este enfoque está evolucionando hacia la gestión de riesgos del ciberespacio (Information Assurance) donde la ciberseguridad consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados... Resumiendo, la ciberseguridad debe formularse proactivamente como un proceso continuo de análisis y gestión de los riesgos asociados al ciberespacio".

Enrique Fojón Chamoro e Ángel F. Sanz Villalba, *Ciberseguridad en España: una propuesta para su gestión* (Madrid: Real Instituto Elcano, 2010), 2.

[4] "Resolution 181, ITU (New)

Through this new resolution, the conference approved the definition of cybersecurity as expressed in Recommendation ITU–T X.1205 as follows:

'Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality'". International Telecommunication Union, "Landmark Decisions from Guadalajara. Cybersecurity", acessado 10 de junho de 2018, http://www.itu.int/net/itunews/issues/2010/09/20.aspx.

[5] Gustavo Diniz and Robert Muggah, *A Fine Balance: Mapping Cyber (In)Security in Latin America. Strategic Paper 2* (Rio de Janeiro: Igarapé Institute, June 2012), 21. https://igarape.org.br/wp-content/uploads/2015/05/A-fine-balance_Mapping-cyber-insecurity-in-Latin-America.pdf.

[6] Para Smith, conforme ressaltado por Fonfria Mesa, a primeira obrigação do soberano era a de proteger a sociedade e que a chave para manutenção da paz entre as nações em um regime de livre comércio era a dissuasão.

Antonio Fronfía Mesa, "Sobre La Naturaleza y Alcance de la Economía de la Defensa" (Madrid: Instituto Español de Estudios Estratégicos, 2016). http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO79-2012_Naturaleza_Economia_Defensa_AFonfria.pdf; Lívia Cardoso Viana Gonçalves, "Ensaio Reflexivo" (Módulo de Economia de Defesa, Colégio Interamericano de Defesa, Washington, DC, janeiro de 2016).

"Las amenazas sobre el ciberespacio se concretan en ciberataques que pueden ser clasificados, en función de su autoría e impacto, según las siguientes categorías: • Ataques patrocinados por Estados. (...). • Terrorismo, extremismo político e ideológico. Los terroristas y grupos extremistas utilizan el ciberespacio para planificar sus acciones, publicitarlas y reclutar adeptos para ejecutarlas. (...) • Ataques del crimen organizado. Las bandas del crimen organizado (ciber-gangs) han comenzado a trasladar sus acciones al ciberespacio, explotando las posibilidades de anonimato que éste ofrece. (...) Según datos del FBI,1 en 2009 el impacto del cibercrimen por la acción de bandas organizadas ocasionó una perdidas, tanto a empresas como a particulares estadounidenses, por un valor superior a 560 millones de dólares. • Ataques

por outro motivo, como ressalta Alejandro Tossi, "cyber threat is one of the main risks for security in development countries".[7]

Os Estados se deparam hodiernamente com grandes desafios tanto âmbito da *elaboração* das políticas públicas, como no que diz respeito a *aplicação* dessas políticas no espaço cibernético. Dentre outros desafios, pode-se destacar a dificuldade em despertar o interesse da sociedade e em se adotar medidas mais efetivas, uma vez que, no geral, há a noção de que defesa e segurança são bens públicos e que devem ser promovidos pelo Estado.[8]

Nessa perspectiva importa destacar outro ponto importantíssimo, e com desdobramentos na estabilidade das relações internacionais, é o desafio em se elaborar políticas adequadas e aumentar as capacidades de defesa sem gerar uma instabilidade internacional com relação aos demais países. Isto porque, as mesmas capacidades adquiridas para ampliar a defesa e segurança cibernética de um país, podem ser empregadas para o ataque. Esta característica, por sua vez, tem o potencial promover uma certa corrida entre os países na ampliação dessas capacidades que podem ter utilização dual, defensiva e ofensiva.

A referida instabilidade poderia ser mitigada na medida em que a elaboração de políticas de segurança cibernética ocorra de forma clara e seja acompanhada de medidas

de perfil bajo. Este tipo de ataques son ejecutados, normalmente, por personas con conocimientos TIC que les permiten llevar a cabo ciber-ataques de naturaleza muy heterogénea y por motivación, fundamentalmente, personal". Fojón Chamoro e Sanz Villalba, *Ciberseguridad en España: una propuesta para su gestión*, 3.

[7] "La evidencia internacional demuestra que los ataques más importantes son 'denegación de servicio' contra redes gubernamentales y sitios web de empresas privadas para interrumpir o deshabilitar su funcionamiento normal; ataques destinados a borrar o destruir información vital en entidades privadas o estatales y ataques para degradar o alterar sistemas de control industriales". Alejandro Amigo Tossi, "Consideraciones sobre la ciberamenaza a la seguridad nacional", *Revista Política y Estrategia* 125 (2015): 87.

[8] Fonfira Mesa, ressalta que para Smith Defesa e segurança não seriam bens a disposição do mercado, mas sim algo que cumpriria ao Estado prover. Isso, por consequência, levaria a caracterização de D&S como sendo de caráter público, bem público, financiado pela imposição, com características de 'não rivalidade, não consumo e não exclusão'. Antonio Fronfía Mesa, "Sobre La Naturaleza y Alcance de la Economía de la Defensa". Como consequência, a não exclusão e não rivalidade de benefícios da característica de Defesa como bem público, levaria, segundo à visão de Patrice Franko uma maior dificuldade em se "produzir defesa mais eficiente". Patrice Franko, *La Economía de la Defensa: Introducción* traduzido por o Colégio Interamericano de Defesa como *A Economia da Economia da Defesa: Introdução* (Waterville, ME: Colby College, 2000),1.

de transparência, que fomentem a confiança de forma sustentável e crescente entre os países.[9]

No âmbito da *aplicação* das Políticas Públicas, por sua vez, importa pensar em como promover a efetividade das normas regulatórias para alcançar todos os agentes se "algunos Estados han utilizado hackers de orientación nacionalista y hacktivistas para ocultar su responsabilidad y evitar la consiguinte abribuicón".[10]

Neste ponto, a dificuldade do gerenciamento do espaço cibernético decorre em grande parte do anonimato que envolve as ações nesse setor, que dificultam sobremaneira a identificação e atribuição de responsabilidades, aspecto que amplia a instabilidade não somente em âmbito internacional, mas também no âmbito interno de cada País.

Destaca-se também que, no momento da aplicação das políticas públicas, há a necessidade da sensibilização/educação dos usuários/agentes no espaço cibernético, uma vez que isso pode gerar vantagens incontáveis, próprias de uma ação preventiva, bem como auxiliar em eventual responsabilização ante ao mau uso, doloso ou culposo, em uma atuação repressiva.

Assim, dentro da enorme complexidade já apontada, cada país procura identificar suas prioridades em doutrinas/paradigmas/approach à luz de suas necessidades e capacidades disponíveis. Alguns países dão maior enfoque à segurança nacional (foco na proteção de infraestrutura crítica e sua importância para atuação governamental), outros mais voltados à economia ou saúde pública. [11]

---

[9] Tossi, "Consideraciones sobre la ciberamenaza a la seguridad nacional", 88.

[10] Tossi, 86.

[11] "All nations address in their NCSS [Australia (AUS), Canada (CAN), Czech Republic (CZE), Estonia (EST), France (FRA), Germany (DEU), India (IND), Japan (JPN), Lithuania (LTU), and Luxembourg (LUX). Romania (ROU), The Netherlands (NLD), New Zealand (NZL), South Africa (ZAF), Spain (ESP), Uganda (UGA), the United Kingdom (GBR; 2009 and 2011 versions), and the United States (USA), of which three (CZE, IND, ROU) are draft NCSS] the cyber threats to their C(I)I. Sixteen nations address this in an explicit manner. Fourteen nations consider the cyber threats as part of their national security of which nine nations mention this explicitly. (…) The threat of loss of public confidence in the use of ICT is explicitly recognised by six of the 18 nations (…) All nations except Japan and the USA explicitly pinpoint individuals, criminals, and organised crime as malicious threat actors. Cyber espionage (e-spionage) is explicitly mentioned by ten nations. Thirteen nations identify the threat of hostile activities by foreign nations (e.g., cyber warfare) in their NCSS. (…) Thirteen nations fear (potential) cyber attacks by terrorists on their C(I)I, (…) Eight NCSS put a focus on the economic prosperity of the digital society. Eight nations put a focus on the confidence of the citizens and companies of the digital society. (…) ten of the 18 nations relate the content of their NCSS to guiding principles or framework conditions. (…) Eight nations refer to the protection of civil liberties and other (inter)national democratic core values.(…) . Eight nations refer to cooperation and public-private partnerships (PPP) as a cyber security framework condition. Only eight nations have defined the notion cyber security. The other

Quanto da utilização de enfoques econômicos é possível se adotar um sistema de incentivos aos usuários/atores do sistema para alcançar seus objetivos, como, por exemplo, a concessão de bônus pecuniário ou fiscal para aqueles que adotam medidas preventivas de segurança, tal como ocorre com empresas seguradoras de veículos automotores. Ou ainda, os países podem adotar medias para reduzir/subsidiar o valor do software utilizado para os sistemas de segurança com o fim aumentar a segurança do sistema como um todo.

Todavia, esse enfoque tem como fragilidade a dificuldade em determinar os custos da insegurança e determinar as externalidades associadas à falta de correlação direta entre o gasto com segurança e o efetivo aumento de segurança sistêmica. Ademais muitas empresas não relatam de forma imediata as falhas de segurança no sistema com receio de sofrer perdas econômicas, o que tendem a ampliar ainda mais os danos.

O enfoque em bem público/saúde pública por sua vez, parte da natureza inafastável de que defesa e segurança como bens, ainda que no espaço cibernético, continuam a ser um bem público.[12] Nesta condição, os desafios para sua proteção/promoção seguem os mesmos daqueles existentes nos demais domínios. Isto porque, como bem aproveitado por todos de forma indistinta, não há grandes incentivos e a população, por achar que o Estado é o grande responsável, tende a atuar como *free rider*. O Estado, neste caso, deve desenvolver standards mínimos e outras ações

ten nations either use descriptive text in their NCSS or a kind of common public understanding. This may cause misunderstandings nationally and internationally. As nations lack a harmonised cyber terminology. (…) the NCSS are relatively weak when describing detailed action plans under the topic 'international collaboration'. (…) Most NCSS lack a dynamic approach to cyberspace (technological) threats and challenges; (…) When it comes to tactical and operational plans, only three nations use some of the SMARTness criteria. (…) Given the global threat, sense of urgency and the need for swift action, transparency is required for all stakeholders. Therefore, we recommend a SMART definition for all NCSS action lines and planned activities. Most NCSS recognise the need for a society-wide approach: citizens, businesses, the public sector, and the government. However, the set of actions aimed at citizens is most often limited to awareness campaigns and information security education at schools. Only Australia has an outreach programme which supports the citizens with national cyber security tools. (…) most nations underrate the risk of loss of public confidence in ICT which may seriously hamper economic prosperity and e-government plans". Eric Luiijf, Kim Besseling, and Patrick De Graaf, "Nineteen National Cyber Security Strategies", *International Journal of Critical Infrastructures* 9, no. 1 (January 1, 2013): 3–31. doi:10.1504/IJCIS.2013.051608.

[12] Sobre o tema interessantes informações pode ser encontradas no seguinte artigo: Scott Charney, "Collective defense: Applying the Public-Health Model to the Internet", *IEEE Security and Privacy* 10, n.2 (March-April, 2012): 54-59.

similares que permitam promover a "saúde pública" do espaço cibernético. [13]

Neste ponto, a título exemplificativo, dentro de uma categorização mais aberta de índole predominantemente didática, considera-se que a abordagem adotada pelos Estados Unidos e Inglaterra estaria orientada à segurança nacional e economia; Jamaica e Trinidad Tobago um enfoque econômico, mas também com motivação na perspectiva de segurança; e Panamá com maior atenção nas infraestruturas críticas.[14]

Poder-se-ia dizer que o Brasil teria adotado uma abordagem de segurança cibernética com enfoque em segurança nacional e defesa, mas também como importante fator de estabilidade social, por meio da defesa dos ativos de informação e das infraestruturas críticas.[15]

Reitere-se, embora cada país adote perspectivas diferentes, segundo suas realidades, nota-se uma certa tendência em se considerar as ameaças cibernéticas como parte da segurança nacional, embora não seja usual a adoção de uma definição clara sobre segurança cibernética ou a elaboração de planos operacionais para o manejo de situações de crise.

Nota-se assim, em uma perspectiva mundial, a existência de uma diversidade enfoques adotados pelos países (políticas e estratégias), bem como a própria definição

---

[13] Kevin P. Newmeyer, módulo "Cybersecurity do Colégio Interamericano de Defesa", Washington, DC, 5 de fevereiro 2018.

[14] Kevin P. Newmeyer, "Modulo de Cybersecurity" (Powerpoint presentation, Modulo de Cybersecurity, Colégio Interamericano de Defesa, Washington, DC, 12 de fevereiro no curso de ano 2018).

[15] Uma análise mais profunda com relação à abordagem brasileira pode ser melhor realizada quando da observação dos marcos jurídicos que evoluíram desde 2001, dentre os quais importa destacar a Medida Provisória n. 2.216-37, de 31 de agosto de 2001, em especial o art. 6; o Decreto n. 5.772, de 8 de maio de 2006; o Decreto n. 9.031, de 12 de abril de 2017; a Estratégia de Defesa Nacional, Decreto n. 6.703, de 18 de dezembro de 2008,; a Portaria 45, de 2009 do Gabinete de Segurança Institucional; o Decreto 7.809, 20 de dezembro de 2012, que cria o Centro de Defesa Cibernética no âmbito o Exército Brasileiro; a Política Cibernética de Defensa do Brasil de 2012, que destaca a importância da segurança da informação e das comunicações, bem como a necessidade da colaboração ativa da sociedade; o Decreto Legislativo n. 373 de 2013, que atualizou da Estratégia de Defesa, Doutrina Militar de Defesa Cibernética; a Diretriz Ministerial MD31-M-17, de 2014; a a Portaria Normativa 3,010/MD de 18 de novembro de 2014 e Instituição de grupo de trabalho para elaboração de uma Política Nacional de Segurança da Informação em 2017. Os documentos em referência podem ser localizados em seu inteiro teor, em sua maior parte, nos seguintes sites: "Legislação", Governo do Brasil, acessado 18 de junho de 2018, http://www4.planalto.gov.br/legislacao; Ministério da Defesa, *Política Cibernética de Defesa* (Brasília: Ministério da Defesa, 2014). http://idciber.eb.mil.br/images/documentos/doutrina/manual_pol_nac_def.pdf; Ministério da Defesa, *Doutrina Militar de Defesa Cibernética* (Brasília: Ministério da Defesa, 2014), 25. https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.

básica do que vem a ser segurança cibernética.[16] Essa falta de uniformidade, por sua vez, pode ser um problema na medida em que possui o potencial de retardar/impedir a construção de avanços colaborativos no setor.[17]

No continente Americano, embora haja divergência sobre a forma de tratar o tema, verifica-se um certo alinhamento político importante para ampliação da cooperação, que é vital nesta área, mas que, todavia, precisa avançar com aporte específico e continuado de recursos, ampliação de conhecimento e de capacidade técnica.[18]

Nessa perspectiva, a Organização dos Estados Americanos, com base em dados colhidos por um rlatório de 2016, que aponta debilidades nacionais e internacionais, alerta para o fato de que apenas 1 dentre 5 países no continente americano tem uma melhor preparação no setor cibernético. Destaca, ainda, que, dentro de um espaço amostral de 32 países analisados: 2 países possuem cidadãos com consciência das ameaças cibernéticas e importância para de sua segurança, 5 países têm estratégias elaboradas, e 8 possuem sistemas de coordenação em caso de ataque a Infraestrutura. Esse diagnóstico nos alerta para uma situação de fragilidade, que precisa ser melhor

[16] Embora não seja possível encontrar na literatura existente uma definição única sobre segurança cibernnética dada a natureza multidisciplinar, Dan Craigen elaborou seguinte conceito: "We propose the following definition, which integrates key concepts drawn from the literature and engagement with the multidisciplinary group: Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights". Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, "Defining Cybersecurity", *Technology Innovation Management Review* 4, no. 10 (October 2014): 17. https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf.

[17] "The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity potentially impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges". Craigen, Diakun-Thibault, and Purse, 13.

[18] "En términos globales, los Estados miembros de la OEA han mostrado unidad cuando se trata de asuntos de Ciberseguridad... adoptado por unanimidad la Estrategia Interamericana Integral de Ciberseguridad nueve años antes, en 2004. una declaración sobre el "Fortalecimiento de la Ciberseguridad en las Américas" en marzo de 2012. La adopción de estos documentos prueba que aunque todavía queda mucho por hacer y los Estados intercambian distintas opiniones sobre la mejor forma de lograr la Ciberseguridad, existe un consenso político sólido en el Hemisferio Occidental, lo que ayuda a facilitar la cooperación regional y el intercambio de información. (...) Muchos gobiernos empezaron a tomar medidas serias para fortalecer la Ciberseguridad, tras la adopción de la Estrategia de Ciberseguridad de la OEA en 2004. En términos generales, los dirigentes políticos son conscientes de los peligros que plantean los hackers y los delincuentes cibernéticos para el desarrollo y la seguridad pública. Sin embargo, la voluntad política no siempre conduce a cambios en la situación imperante. En Latinoamérica, dos factores bloquean comúnmente los esfuerzos de los estados miembros: • La falta de recursos dedicados al fortalecimiento de la capacidad en Ciberseguridad. • La escasez de conocimientos especializados y experiencia práctica para la implementación de políticas y capacidades técnicas". Leiva, "Estrategias Nacionales de Ciberseguridad", 168.

estruturada.[19]

Neste sentido, é possível identificar a importância da construção de abordagens comuns entre os Estados, que sejam inclusivas e interdisciplinares, e que tenham: a) clareza das debilidades, b) identificação dos riscos na promoção de desenvolvimento e do interesse nacional, c) um sistema normativo inteligente e operativamente flexível, que reflitam estratégias adequadas segundo os principiais atores e cenários, e d) atenção especial às infraestruturas críticas, pois, conforme destaca Kevin Newmeyer, "Critical infrastructure protection should be a key aim of the national cybersecurity strategy. Establishment of minimal standards is necessary in an economic or public health model of cybersecurity".[20]

Como conclusão parcial, destaca-se que, destarte as ameaças cibernéticas sejam percebidas de diferentes formas pelos atores (inclusive agentes estatais), e isso reflete em diferentes formas em se abordar o problema, não há uma estratégia melhor que outra. O importante é que se busque uma abordagem integral/interdisciplinar, sem deixar de considerar uma questão de peculiar importância nesta temática, aquela relativa à proteção de infraestruturas críticas, que será tratada de forma mais específica em tópico posterior.

Trata-se de buscar a construção de uma visão elaborada pela participação de tantos quanto numerosos os atores e que seja garantidora dos aspectos centrais da segurança individual e nacional, que pode aumentar a eficácia das políticas e estratégias de segurança cibernética.

II. Importantes aspectos de um marco regulatório eficiente

O espaço cibernético surge como quinto domínio, ao lado dos domínios terrestre, marítimo, aéreo e espacial. Neste novo domínio, criado integralmente pelo homem, é possível identificar debilidades e vulnerabilidades específicas, bem como diferentes ameaças ("online identity theft, industrial cyber espionage, critical

[19] Center for Strategic and International Studies, "Cybersecurity Report 2016: Are We Ready in Latin America and the Caribbean?" March 2016, CSIS Events, 1:49:13. https://www.csis.org/events/cybersecurity-report-2016-are-we-ready-latin-america-and-caribbean.

[20] Kevin Newmeyer, "Elements of National Cybersecurity Strategy for Developing Nations", *National Cybersecurity Institute Journal* 1, no. 3 (2015): 17.

infrastructure protection, and botnets").[21]

Isto é, temos novos e complexos desafios[22] no processo de promoção da segurança pessoal e nacional,[23] em que a solução exige novos paradigmas que contemplem igual complexidade.[24]

A internet, como principal característica desse meio, assegura o tráfego informações incontáveis e conexão de um número inimaginável de pessoas. Embora potencialmente muito positiva para o desenvolvimento e a economia, as características da rede, que permitem o anonimato de ações irregulares, podem afetar inúmeros direitos e que, se não gerenciados de forma adequada, podem, por consequência, impactar no desenvolvimento e economia a que se busca promover.

Conforme os termos dantes destacados, a dificuldade na identificação dos atores, associada a custos de operação/ataque relativamente baixos têm um potencial de promover grandes e incontáveis danos, para os quais todos nós precisamos nos preparar. Isto porque:

> As nossas atuais vulnerabilidades (falta de sensibilidade/educação da população, falta de pessoal com alto grau de capacitação, capacidades limitadas, frágil interação do público/privado) associadas às ameaças cibernéticas (de natureza estatal e não estatal em um contexto em que falta de normatização comum entre os Estados, o que dificulta a responsabilização e punição de crimes) geram uma prospectiva de cenário não muito favorável, instável, cuja dimensão pode afetar a

[21] "Malware is frequently used to steal passwords and compromise online banking, cloud and corporate services". Tyler Moore, "The Economics of Cybersecurity: Principles and Policy Options", *International Journal of Critical Infrastructure Protection* 3, no. 3–4 (December 2010): 2.

[22] "In this paper, we have described several key economic challenges: misaligned incentives, information asymmetries and externalities. We have also reviewed the policy options available for overcoming these barriers, notably information disclosure and intermediary liability. Our principal recommendations are to encourage ISPs to take a more active role in cleaning up infected computers, and to collect and publish data on a range of security incidents. These recommendations are designed to raise awareness of cybersecurity issues and assign responsibility for action by the private sector so that the risks to society may be mitigated". Moore, 23.

[23] "On a global scale, two major trends in cybercrime are fraud with economic motivations, and attacks against confidentiality, integrity and availability". Organization of American States, *Report on Cybersecurity and Critical Infrastructure in the Americas 2015* (Washington, DC: Organization of American States and Trend Micro, 2015), 18.

[24] A tecnologia superou as políticas e nossas políticas muitas estão desatualizadas e, por consequência, as capacidades também. Precisamos construir novos paradigmas não somente tecnicamente eficiente, mas legitimamente fixados, segundo o balanço entre segurança e privacidade que cada pais ira alcancar. Mas o desafio, como se descutir, como se flexibilizar privacidade se não sinto como ameaça. Kevin P. Newmeyer, "Cybersecurity do Colégio Interamericano de Defesa" (Colegio Interamericana de Defesa, Washington, DC, 3 de março de 2018).

> sobrevivência dos Estados.
>
> Nesse cenário, criminosos mediante a utilização de recursos de baixo investimento, podem afetar sociedades não somente pelo impacto em infraestruturas críticas e afetando a economia, afetando prestação de serviços fundamentais, mas também fragilizando o exercício de direitos básicos como intimidade, privacidade e propriedade.
>
> A alternativa à esta situação está em se encontrar formas de: i) se construir maior confiança entre os Estados em compartilhar informações e tecnologias de segurança para a comunidade internacional, ii) promover, entre os Estados e os cidadãos, um balanço legítimo e adequado entre segurança e privacidade, e iii) promover parcerias entre o setor público e o privado, em que embora o setor público oriente, o privado tenha incentivos para cooperar de forma participativa.[25]

Trata-se de uma situação extremamente perigosa que permite o surgimento e o avanço do crime cibernético (delitos comuns que se utilizam o espaço cibernético como meio para realização de seus objetivos, em grande parte econômicos),[26] terrorismo cibernético[27] (as tecnologias da informação são utilizadas para intimidar ou causar dano a grupos sociais, com fins políticos-religiosos)[28] e a guerra cibernética ("Cyber war is just one outcome of the exercise of cyber power between nations")[29] como grandes

---

[25] Lívia Cardoso Viana Gonçalves, "Fórum #2, Módulo Cybersecurity do Colégio Interamericano de Defesa", Moodle, 25 de fevereiro de 2018.

[26]"El concepto de cibercrimen abarca desde el delito económico, como el fraude informático, el robo, la falsificación, el computer hacking, el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión de la intimidad, la distribución de contenidos ilegales y dañosos, la incitación a la prostitución y otras actitudes que atenten contra la moralidad, y el crimen organizado".Gema Sánchez Medero, "Ciberespacio y el Crimen Organizado. Los nuevos desafíos del siglo XXI". *Revista Enfoques: Ciencia Política y Administración Pública* 10, n.16 (2012): 73.

[27] O Convênio de Budapeste de 2001, que trata sobre Cibercrime no âmbito predominante na Europa, não fala de ciber terrorismo, indicando certa carência de um compromisso real no âmbito internacional.

[28] "Los grupos terroristas están utilizando, principalmente, la red para financiarse, reclutar nuevos miembros, adiestrar a los integrantes de las distintas células, comunicarse, coordinar y ejecutar acciones, encontrar información, adoctrinar ideológicamente, promocionar sus organizaciones y desarrollar una guerra psicológica contra el enemigo". Sánchez Medero, "Ciberespacio y el Crimen Organizado", 74.

[29] Sobre guerra cibernética importa observar que no âmbito da Organização do Tratado do Atlântico Norte OTAN: "for NATO cyber war as the focus of concern is a misnomer; the real or potential use of cyber power by nations or terrorist groups should be the principle focus. Cyber war is just one outcome of the exercise of cyber power between nations. The central part of the paper will outline some

ameaças do Século XXI. Especificamente com relação à guerra cibernética, pode-se dizer que, a despeito da regulamentação do âmbito da ONU, a aplicação de inúmeros conceitos típicos à guerra tradicional não pode ser realizada de forma tão simples, e algumas questões ainda estão em aberto.[30]

A título exemplificativo, e avaliando o impacto dessas ameaças em âmbito geral, pode-se ter uma ideia considerar a ampliação, a dimensão potencial em uma perspectiva prospectiva dessas ameaças no Brasil.[31]

O Brasil é o país com o maior número de usuários na América Latina, embora com apenas 59% da população tenha acesso.[32] Isto é, os problemas dantes descritos podem a crescer em uma escala significativa, na medida em que se amplie a integralidade de acesso da população do Brasil de da população mundial em direção ao 100%, sem a respectiva ampliação da adoção de soluções operacionais e estruturais de regulação, em âmbito nacionais e internacionais.

Isto porque, o crescimento do número de usuários, em todo o mundo, não tem sido acompanhado de uma segurança progressiva em igual velocidade. Não somente

of special characteristics that distinguish cyber power from the other elements of national power, and point to some of challenges that these special characteristics present in developing a doctrine of cyber power". Jeffrey Hunker, *Cyber War and Cyber Power: Issues for NATO Doctrine*, No. 62 (Rome: Research Division - NATO Defense College, 2010), 1.

[30] "For example, in cyberspace it is unclear what constitutes a weapon, an act of war, or the use of force necessary to trigger UN Charter protections. Perhaps more importantly, the problem of attribution—necessary for a state's invocation of Article 51's self-defense provisions—is exceedingly difficult in cyberspace, or at least much more so than in traditional military conflicts. Further, under international humanitarian law, the principles of proportionality and the distinction between military and nonmilitary targets are harder to apply in the cyberwar context, especially if states choose to respond to cyberattacks with conventional military force (or to counter military force with cyberoperations). Cyberattacks on the military infrastructure of telecommunications networks in cyberspace might have severe consequences on civilian networks, further complicating assessments of proportionality and distinction even for states making good faith efforts to comply with international humanitarian law. Finally, in the absence of an international cyberspace treaty to define the relevant terms, many of the technical questions regarding the fit between the Charter and international humanitarian law on one hand, and the complexity of cyberwar on the other, remain unanswered." Daniel Abebe, "Cyberwar, international politics, and institutional design", *University of Chicago Law Review* 83 n.1 (Winter 2016): 6-7.

[31] "The challenges that Brazil is facing can be classified in three categories: Budgets for research, development, and innovation (R&D&I); organization and control of current cybersecurity systems; and reduction of the dependence of foreign countries regarding supplies and acquisitions". Organization of American States, *Report on Cybersecurity and Critical Infrastructure in the Americas 2015*, 22.

[32] Agência Brasil, "Brasil é o 4º país em número de usuários de internet", *Exame*, acessado em 14 de junho de 2018, https://exame.abril.com.br/tecnologia/brasil-e-o-4o-pais-em-numero-de-usuarios-de-internet/.

porque os incentivos são diferentes (os incentivos, considerando a natureza do mercado, para desenvolvimento de tecnologias são maiores do que os incentivos/investimentos na área de desenvolvimento de sistemas de segurança), mas também porque há, em muitas pessoas, a falsa impressão de segurança, que limita o maior envolvimento dos atores no processo de participação de elaboração e aplicação das políticas públicas de segurança cibernética.

Significa dizer, embora o Estado deva ser o principal agente na elaboração das estratégias e gestão nacional, ele não pode atuar de forma isolada, pois precisa da participação ativa do setor privado.[33] Para que o sistema funcione é necessária uma forte liderança/vontade política e que essa vontade esteja não somente no momento da elaboração das políticas, mas também em sua aplicação, com recursos e estratégias.[34]

---

[33] A Resolução 174 da International Telecommunication Union (ITU) enfatiza a importância colaboração entre o setor público e privado para prevenir, detectar e responder a cibercrimes e uso indevido da tecnologia em âmbito nacional e internacional, por meio da elaboração de normas que contemplem a atuação do setor público e do privado, que permitam investigar e castigar e, com isso propicie sensibilização, educação no âmbito interno e maior cooperação/diálogo no âmbito internacional. Nesse contexto, a World Summit on the Information Society (WSIS), destacou que a ITU tem o papel de facilitador da linha de ação 5.

"Resolution 174

Illicit use of information and communication technologies could have a detrimental impact on a country's infrastructure, national security and economic development. This new resolution, entitled "ITU's role with regard to international public policy issues relating to the risk of illicit use of information and communication technologies", calls for action to curb such use. It instructs the Secretary-General to raise awareness of Member States regarding the adverse impact that may result from the illicit use of information and communication resources. He should also take the necessary measures to maintain the role of ITU to cooperate within its mandate with other United Nations bodies in combating the illicit use of ICT.

In this regard, the resolution underlines the importance of the outcomes of the World Summit on the Information Society (WSIS), in particular, the role of ITU as facilitator for WSIS Action Line C5 on building confidence and security in the use of ICT. It recalls that WSIS Action Line C5 stipulates that: "Governments, in cooperation with the private sector, should prevent, detect and respond to cybercrime and misuse of ICT by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of such misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness". International Telecommunication Union. "Landmark Decisions from Guadalajara".

[34] "Propuestas para... gestión eficaces y eficientes de nuestra (Espanha) ciberseguridad... se deberían aplicar los siguientes principios: (1) El gobierno de España debe identificar la seguridad de su ciberespacio como un objetivo estratégico de la Seguridad Nacional... (2) Se debe elaborar una Estrategia Nacional de Ciberseguridad de la que emane un marco normativo específico que regule el ciberespacio y su seguridad. (3) La dirección de la ciberseguridad debe realizarse de manera centralizada... coordinando a las entidades públicas y privadas implicadas. (4) El gobierno debe fomentar y reforzar la cooperación internacional en materia de ciberseguridad... (5) Las administraciones del Estado se deberán promover una cultura de la ciberresponsabilidad, basada en la concienciación y formación continua en ciberseguridad... (6) El Estado debe promover e invertir en la investigación, el desarrollo y la innovación (I+D+i) del sector de la ciberseguridad, que proporcione soluciones TIC de primer nivel y empleo cualificado... Todos son corresponsables, pero le corresponde al gobierno el liderazgo y la dirección de la

Nesse contexto, como se trata de um problema do todo governo (em diferentes esferas), e de toda sociedade, mister se faz a identificação de um ponto focal para coordenar as ações interestatais e as ações entre o setor público e privado, e, assim, construir a confiança necessária a todo processo.[35] Para tanto, é preciso a elaboração de um marco legal que oriente toda administração, como política pública, incluindo também o setor privado.[36]

É importante existir no setor cibernético uma relação de sinergia em que as empresas colaboram ao agregar valor de sua atuação e o Estado investe em tecnologia para "bidireccional: las empresas necesitan crear valor alrededor del negocio de la ciberseguridad y el Estado precisa de tecnología que le permita disponer de una capacidad solvente y vanguardista de ciberseguridad".[37]

No Brasil, essa relação encontra-se em processo de considerável evolução, e tem representado incremento progressivo se comparado à América Latina.[38] Importante

gestión nacional de la ciberseguridad". Fojón Chamoro e Sanz Villalba, *Ciberseguridad en España: una propuesta para su gestión*, 7-8.

[35] Neste ponto cabe de forma adicional destacar que, segundo Levia, as Estratégias de cybersecurity devem ter "d) Participación del sector privado: Participación en la estrategia/política: los actores en sectores claves como energía, transportes, entidades financieras, bolsas de valores, proveedores de servicios de internet, entre otros deben evaluar los riesgos que los afectan y mediante una adecuada gestión de los mismos asegurar que los sistemas de información y las redes son fiables y resistentes. Además deben asumir el compromiso de compartir la información con las autoridades gubernamentales competentes en materia de Ciberseguridad". Leiva, "Estrategias Nacionales de Ciberseguridad", 164.

[36] Kevin Newmeyer, "Elements of National Cybersecurity Strategy for Developing Nations", 17.

[37] Fojón Chamoro e Sanz Villalba, *Ciberseguridad en España: una propuesta para su gestión*, 6.

[38] "Indeed, Latin American countries are largely absent from wider strategic international debates on cyberspace. According to Camino Kavanagh, with the exception of Brazil, Latin American countries are not actively involved in discussions on internet freedom, internet governance or wider UN debates. For its part, Brazil is largely working on related issues through the India-Brazil-South Africa forum. Interview, May 2012. There is comparatively less publicly available evidence of bilateral cooperation between Latin America countries on managing cyber-security and cyber-defense. While this is a possible area of growth, just one country has signed a treaty – Brazil – with another country outside of Latin America – Russia". Diniz and Muggah, *A Fine Balance*, 10. "A growing number of Latin American countries have elaborated specific legislation on cyber-crime. Using these criteria, there are at least six Latin American countries reviewed in the preparation of this Strategic paper that have yet to develop clear and specific laws to penalize cyber-crimes – Belize, Brazil, Cuba, El Salvador, Honduras and Nicaragua". Diniz and Muggah, 12. "One important exception at the regional level is the non-governmental organization *Latin American Cooperation of Ad- vanced Networks* (RedCLARA), which seeks to connect institutions working on the issue of cyber security. Specifically, RedCLARA connects 15 Latin American academic networks, such as Brazil's RNP (*Rede Nacional de Pesquisa e Ensino*) and Peru's RAAP (*Red Académica Peruana)*". Diniz and Muggah, 17. "In Latin America, private corporations and firms appear to be playing a comparatively marginal role in supporting cyber- security initiatives and enhancing public safety in cyber-space. Not a single public-private partnership could be

registro dessa evolução e atuação colaborativa com a sociedade é a Política de Defesa Cibernética, Portaria n. 3.389, de 21 de dezembro de 2012.[39] Todavia, estudiosos sobre o tema, como Gustavo Diniz ressaltam algumas dificuldades na cooperação do setor privado com o setor público.[40]

Com esses aspectos, uma maior eficiência das políticas de segurança cibernética passa também pela definição de um marco legal apropriado, como elemento de educação, dissuasão e incentivos de modo flexível *(smart regulation)* no âmbito interno,[41] e elemento de cooperação e formação de uma defesa coletiva no âmbito interno e externo.[42]

---

identified in the course of the preparation of this Strategic paper in Latin America. (…) Most are reluctant to share information on the scale of their losses to federal or district level authorities. As noted in the *Security and Defense Agenda's* report: "[t]he problem is that companies are reluctant to talk about these (cyber-crime issues); they aren't keen to reveal vulnerabilities to competition or to consumers, and they also have data privacy rules to contend with.(..) It should be stressed that a major assessment of the overall engagement of the private sector on issues of cyber-security in Latin America found that its standards and participation were "marginal to poor" when compared to those of other regions.63 both public and private responses to cyber threats in selected Latin American countries are rated as poor according to governmental and industry standards set by groups such as PriceWaterhouseCoopers and the Security and Defense Agenda". Diniz and Muggah, 19.

[39] Destaque-se, dentre outros dispositivos desse documento, o item "3.1.2 A eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa. Nesse contexto, avulta de importância a necessidade de interação permanente entre o MD e os demais atores externos envolvidos com o Setor Cibernético, nos níveis nacional e internacional, conforme estabelece a END". Ministério da Defesa, *Doutrina Militar de Defesa Cibernética*, 25. https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.

[40] "The URCC (The Federal Police's Unit for Combating Cybercrime) appears to be operating effectively in terms of exchanging information on operational matters with foreign law enforcement agencies and courts. In contrast, when a case requires the cooperation of private Internet companies in the US, including Google and Facebook, there are often long delays and obstructions. These companies tend to avoid collaborating with law enforcement due to contractual and legal obligations in the countries that host their core services and servers."

Gustavo Diniz, Robert Muggah and Misha Glenny, *Deconstructing Cyber Security in Brazil: Threats and Responses. Strategic Paper 11* (Rio de Janeiro: Igarapé Institute, December 2014), 22. https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf.

[41] "Must focus on the costs of ensuring Internet health. (…) Industry and government should identify the level of security that markets will naturally provide. Regulation would create processes to fill the gap between what markets will naturally provide and what national security requires. The government's tool kit for this change should be viewed as expansive and flexible, including the use of policy and economic incentives to reinforce or supplant regulation". Charney, "Collective defense", 58.

[42] Charney: "Partners across the computing ecosystem, including the IT industry, ISPs, and governments, must help foster greater collective defense. Collectively, we can help develop and promote the expected actions and behaviors that will improve Internet safety. (…) We can also begin working through international bodies to standardize what types of information on machine health to share and how to exchange it with appropriate security and privacy protections. As more efforts advance, we can create

Trata-se de um aspecto essencial para conscientização de todos os agentes, sobre seus deveres, para que usem de forma adequada como *public health*, com direitos para tenha as liberdades civis asseguradas, bem como para, no âmbito público, orientar de forma coordenada os órgãos públicos. Esse marco regulatório dever, ainda, estabelecer metas para desenvolvimento das capacidades (físicas e profissionais) adequadas,[43] acompanhado de um plano operacional segundo estratégias setoriais e recursos dedicados.[44]

Isto é, uma política de segurança cibernética eficiente requer um marco legal que permita a conscientização e incentive a participação dos atores (nacionais e internacionais, estatais e privados) de forma participativa, colaborativa. Caso contrário, não seremos capazes de atuar contra o crime cibernético e o terrorismo cibernético, bem como evitar escaladas das guerras cibernéticas.

III.Importância da proteção às Infraestruturas Críticas

Vivemos em uma aldeia global em que todos estamos conectados, mas não por uma mera nuvem, mas também por um meio físico. Nossa relação real está cada vez mais conectada com a internet e envolvida pela tecnologia da informação, e qual é nossa visão crítica atual? [45] A internet mudou nossa relação com a realidade física, mas sabemos a natureza e amplitude de que impactos no espaço cibernético podem causar no

guidelines to catalyze further action. We must also drive the R&D that will remove barriers to, lower costs for, and incentivize toward the right actions and behaviors. Finally, we can advocate the necessary policy and legislation reform to enable and eventually transition to a state in which collective defense and consumer endpoint health management aren't just feasible, but a reality".

[43] Kevin Newmeyer, "Elements of National Cybersecurity Strategy for Developing Nations", 17.

[44] "Apuesta por promover la cooperación con las comunidades autónomas e impulsar un foro social de expertos como órgano consultivo. Asimismo, pide actualizar los instrumentos normativos necesarios, especialmente en lo referente a la gestión de las situaciones de crisis, la protección civil, los secretos oficiales y el planeamiento frente a emergencias y catástrofes. Además, se establecerá una Comisión Coordinadora para luchar contra el crimen organizado y se elaborarán estrategias sectoriales, entre las que cita una sobre ciberseguridad". Maria José Caro Bejarano, *La Protección de las infraestructuras críticas* (Madrid: Instituto Español de Estudios Estratégicos, 2011), 6. http://www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf.

[45] Andrew Blum, "Discover the physical side of the Internet", June 2012, TEDGlobal. http://www.ted.com/talks/andrew_blum_what_is_the_internet_really

mundo real? [46] Fato é que, os ataques cibernéticos podem causar danos reais, com especial atenção em infraestruturas críticas e precisamos nos adaptar rapidamente a essa realidade.

As respostas aos questionamentos anteriores, em geral, revelam um baixo conhecimento do público geral, isso, por sua vez, tem o potencial de gerar problemas de ordem multidimensional no âmbito individual e nacional.

Neste ponto, um dos aspectos mais sensíveis está relacionado à proteção das infraestruturas críticas.[47] Isso porque elas são vitais à política de segurança cibernética e tem potencial de criar enormes danos.[48]

A despeito do Brasil ter um tratamento normativo específico com relação à infraesturutura crítica (dentre outras, a Portaria n. 45 de 8 de setembro de 2009,[49] que destaca essas infraestruturas como foco de proteção da Segurança Cibernética) e haja ações concretas para fortalecer essa proteção, a OEA pôde identificar impactos no Brasil, México e na Colômbia,[50] bem como desafios comuns a outros países.[51]

---

[46] Goldstein ilustra de forma bem interessante como os ataques cibernéticos podem impactar no mundo físico e como conflitos no âmbito digital tem potencialidade que provocar conflitos armados.

Guy-Philippe Goldstein, "How Cyberattacks Threaten Real World Peace", Paris in January 2010, TEDxParis. https://www.ted.com/talks/guy_philippe_goldstein_how_cyberattacks_threaten_real_world_peace.

[47] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, § 1016. USA Patriot Act 2001: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". Cada país elenca o considera ser infraestrutura crítica, mas o Professor Newmeyer destaca alguns pontos em comum, quais sejam: "Important to the nation's economy and security, Provide vital services to population, increasingly reliant on IT systems". Kevin P. Newmeyer, "Cybersecurity do Colégio Interamericano de Defesa" (Colegio Interamericana de Defesa, Washington, DC, 3 de março de 2018).

[48] "A estas infraestructuras les puede afectar entre otros, el terrorismo, la inseguridad económica y financiera, la vulnerabilidad energética, las ciberamenazas. 'Es preciso garantizar su funcionamiento y capacidad de resistencia y recuperación ante posibles amenazas'". Caro Bejarano, *La Protección de las infraestructuras críticas*, 6.

[49] Presidência da República. Casa Civil. *Diário Oficial da União – Seção 1* (Brasília: Imprensa Nacional, 9 de setembro de 2009). http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/2009.

[50] "Recent data shows that the cost of cybercrime has reached $8 billion in Brazil, $3 billion in Mexico, and $464 million in Colombia. (...) an increased number of cyber-attacks: owners and operators surveyed for the 2015 OAS-Trend Micro report Cybersecurity and Critical Infrastructure in the Americas reported a 53% increase of cyber incidents affecting their computer systems over the previous year". Organization of American States, *Report on Cybersecurity and Critical Infrastructure in the Latin American and Caribbean 2018* (Washington, DC: OAS, 2018), 8. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/cipreport.pdf.

[51] A esse respeito cabe ressaltar que segundo report da OEA: "America is in Brazil. In addition, Brazil is the first country in Latin America, and the seventh in the world, that invest[s] the most in ITC; investment reached €48.2 billion in 2013. Cybersecurity is one of the key priorities of the National Defense Strategy. This document is inclusive, and it doesn't just covers military matters but also the

Ainda segundo uma visão mais ampla do continente, a OEA destaca que "Data from Brazil, Chile, and Mexico reveals that most of the vulnerabilities are related to the wrong system configurations, followed by outdated versions and application problems. However, those problems are associated with a higher risk level. 60% of vulnerabilities that expose holes could affect information confidentiality. 30% of vulnerabilities represent a threat against integrity, while 10% of vulnerabilities are weaknesses that can take advantage of attacks against the availability of information and services".[52]

Partindo de uma perspectiva técnica, é possível de dizer que, é comum que muitas dessas infraestruturas adotem o sistema SCADA[53] , que não estão conectadas à internet. Essa característica poderia dar certa segurança, mas hoje sabemos que esta segurança é apenas teórica. Isto porque, o fato de uma nfraestrutura não estar conectada à internet não foi suficiente para afastar a utilização de uma poderosíssima arma cibernética, o STUXNET.[54] O Stuxnet foi uma arma composta:

protection of Brazilian critical infrastructures of the space, ITC and nuclear industries, with the aspiration to reduce the dependence on other countries. Brazil has a wide network of early alert centers and response teams against security incidents. The challenges that Brazil is facing can be classified in three categories: Budgets for research, development, and innovation (R&D&I); organization and control of current cybersecurity systems; and reduction of the dependence of foreign countries regarding supplies and acquisitions... Governments and enterprise should basically promote an all-level cybersecurity culture that fosters threat prevention. International and domestic collaboration between the public and private sectors play a key role in strengthening national cybersecurity frameworks. It is necessary to put in more legislative and regulatory work if progress is expected. Information exchange and operational response should be decisive as well". Organization of American States, *Report on Cybersecurity and Critical Infrastructure in the Americas 2015*, 22.

[52] Organization of American States, 18.

[53] Segundo lições do Professor Kevin Newmeyer, SCADA, Supervisory, Control, and Data Acquisition se define como "These circuits control the switches, valves, signals, etc. that are embedded in everything from subway systems to electrical distribution, to traffic lights. Connected to the Internet, they allow remote monitoring and control of systems". Todavia, considerando que a maior parte desses sistemas que estão em utilização são da década de 80, são sistemas em grande parte desatualizados e não conectados à internet, embora em versões modernas isso seja possível. Kevin P. Newmeyer, "Cybersecurity do Colégio Interamericano de Defesa" (Colegio Interamericana de Defesa, Washington, DC, 3 de março de 2018).

[54] "Stuxnet infects Windows systems in its search for industrial control systems, called supervisory control and data acquisition (SCADA) systems. The target systems include code that automates industrial machinery (Falliere, 2010). A majority of the infected computers worldwide were located in Iran, with uranium enrichment factories as the supposed target of the Stuxnet worm (Fildes, 2010). Stuxnet was first observed and spread in early 2010, but the roots were traced back roughly to June 2009. The Russian cyber-security company Kaspersky Lab claimed that the attack could only be conducted with nation-state support (Fildes, 2010). The most likely origin of the virus seems to be either Israel or the United States, though the origin remains disputed (Keizer, 2010). Israeli officials have hinted that their country may be involved (Broad et al., 2011). Iran's top nuclear negotiator blamed the United States and claimed that an investigation found that the United States was the source of the attack". Nazli

> por duas bombas digitais, uma voltada para acelerar as turbinas de enriquecimento de urânio do Irãn e outro um Rootkit voltado para camuflar o ataque e, com isso, retardar a resposta da vítima, ampliando os danos no sistema. Isso foi possível graças à exploração do Zero day, que infectou um computador, cujo software controlava o SCADA. Todavia, depois que infectado o sistema, o malware atuava como Selfreplicating worm. Por essa razão se acredita que embora tenha sido um ataque direcionado ao Iran, acabou por atingir outros países como a India e Indonésia, dentre outros. A infecção inicial ao computador ocorreu por meio da utilização de pen drive, e o vírus tinha características tão específicas que deixa evidente que quem criou o malware não somente tinha muita capacidade tecnológica (especialistas dizem que somente Estados poderiam dispor de tal capacidade), mas conhecia profundamente o *modus operandi* do sistema utilizado na matriz energética do Iran. Tratar-se-ia de um malware que carrega uma tecnologia 20 vezes maior daquela até então utilizada, alguns comparam sua grandeza ao advento da internet.[55]

Este malware atingiu centrífugas de enriquecimento de urânio no Irã. A tecnologia utilizada indica a criação por um ou mais Estados, como uma manifestação de uma guerra cibernética. "Stuxnet has effectively fired the starting gun in a new arms race (…) Unlike nuclear or chemical weapons, however, countries are developing cyberweapons outside any regulatory framework".[56] Com esse exemplo, é possível verificar uma dissuasão diferenciada da guerra fria,[57] a utilização de uma arma cibernética pode se voltar contra seu próprio criador.[58]

Instaura-se uma nova racionalidade, a qual não temos ainda exata dimensão ou controle, uma vez que fogem à tradicional governança instaurada à luz do Tratado de

---

Choucri and Daniel Goldsmith, "Lost in cyberspace: Harnessing the Internet, international relations and global security", *Bulletin of the Atomic Scientists* 68, n.2 (2012): 76-77. doi:10.1177/0096340212438696.

[55] Cardoso Viana Gonçalves, "Ensaio Reflexivo", 21.

[56] Misha Glenny, "A Weapon We Can´t Control", *New York Times*, junho 24, 2012, acessado em 31 de março de 2018, http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html.

[57] "During the cold war, countries' chief assets were missiles with nuclear warheads. Generally their number and location was common knowledge, as was the damage they could inflict and how long it would take them to inflict it. Advanced cyberwar is different: a country's assets lie as much in the weaknesses of enemy computer defenses as in the power of the weapons it possesses. So in order to assess one's own capability, there is a strong temptation to penetrate the enemy's systems before a conflict erupts". Glenny, "A Weapon We Can´t Control".

[58] Veja: Sean Collins and Steven McCombie, "Stuxnet: the emergence of a new cyber weapon and its implications", *Journal of Policing, Intelligence, and Counter Terrorism* 7, n. 1 (2012). https://www.tandfonline.com/doi/citedby/10.1080/18335330.2012.653198?scroll=top&needAccess=true.

Westfalia -1648, com as concepções correntes sobre Estado, territorialidade, soberania e não intervenção.

Essa nova racionalidade, ou irracionalidade, preocupa na medida em que "in cyberspace; once released, virus developers generally lose control of their inventions, which will inevitably seek out and attack the networks of innocent parties. Moreover, all countries that possess an offensive cyber capability will be tempted to use it now that the first shot has been fired".[59]

Temos assim um grande desafio, que é global, o de regular e construir um espaço seguro e de confiança em que os incentivos ao uso das armas cibernéticas sejam menores do que as possíveis responsabilizações/sanções no âmbito internacional. A resposta não é fácil, uma vez que embora haja iniciativas, elas ainda não se mostram muito eficientes.[60]

Neste ponto, Leiva destaca a importância da "elaboración y adopción de estándares globales, la expansión de la capacidad del sistema jurídico internacional y el desarrollo y la promoción de las mejores prácticas para generar sistemas de alerta y de respuesta a los ciberataques".[61]

No âmbito das Américas é possível ver algumas dessas inciativas como a "Declaration Strengthening Cyber-Security in the Americas" de 2012[62] do programa de Cybersecurity da CICTE Inter-American Committee against Terrorism[63] e a inclusão do tema na agenda de discussões da UNASUL.

Todavia, subsistiria, na perspectiva da Organização dos Estados Americanos, algumas limitações quanto à "Budgets for research, development, and innovation (R&D&I); organization and control of current cybersecurity systems; and reduction of

[59] Glenny, "A Weapon We Can´t Control".

[60] Embora stuxnet tenha sido um ato contra as leis internacionais (por ser um worm selfreplicating, não discriminatório alcançando civis) a dificuldade de atribuição do ataque e a falta de reconhecimento do Iran tornaram mais difícil a regulação internacional.

[61] Leiva, "Estrategias Nacionales de Ciberseguridad", 164.

[62] Organization of American States, *Declaration. Strengthening Cyber-Security in the Americas*, CICTE/DEC.1/12 rev. 1, (Washington, DC: Member States of the Inter-American Committee Against Terrorism (CICTE), March 7, 2012). https://www.oas.org/en/sms/cicte/Documents/Declarations/DEC_1%20rev_1_DECLARATION_CICTE00749E04.pdf.

[63] "The OAS/CICTE Cybersecurity Program serves a pivotal role in fostering the public-private partnership that is still maturing in the region. It is in the spirit of such a public-private partnership that OAS and Trend Micro joined forces to provide you with this unique perspective into critical infrastructure attacks that have impacted 25 nations. Collective action is direly needed". Organization of American States, *Report on Cybersecurity and Critical Infrastructure in the Americas 2015*, 46.

the dependence of foreign countries regarding supplies and acquisitions".[64]

A análise, ainda que superficial, do caso Stuxnet permite perceber a importância da elaboração de recomendações claras ao se tratar de infraestruturas críticas para todos os atores envolvidos, tal como a criação de estândares de segurança no setor industrial no contexto de estratégias que reforcem a confiança entre os Estados e permitam a rápida resposta no âmbito político e técnico.[65]

Por tais aspectos, podemos notar que os ataques cibernéticos podem causar danos reais, especialmente em infraestruturas críticas. Atualmente, graças à natureza do ataque cibernético e limitação do ordenamento internacional, temos uma insegurança jurídica que favorece a escalada de conflitos. Precisamos estar preparados para essa realidade, nos adaptar com atuação coordenada e integrada, tanto no âmbito político como técnico.

IV. Conclusão

"What we see, know, and understand today in the cyber domain may not be the same realities of tomorrow".[66] Os desafios que hoje conseguimos identificar no âmbito da segurança multidimensional já são inúmeros e preocupantes na medida em que necessitam de uma resposta interdisciplinar e colaborativa.

O problema, contudo, é que a identificação de interesses no âmbito nos países não é algo tão fácil quanto outrora, uma vez que a globalização e o avanço tecnológico criaram uma nova racionalidade que exige a elaboração de novos paradigmas.

Fica então o grande questionamento: uma vez identificado o grande problema/desafio no mundo cibernético, como atuar?

Neste artigo colacionei várias perspectivas e acredito que esse seja um início,

[64] Organization of American States, 22.

[65] "Promover campañas de educación básicas y orientadas en infraestructuras críticas. Es necesario invertir en seguridad cibernética. Actualización de las estrategias cibernéticas y fortalecimiento de las capacidades para responder legalmente a ataques cibernéticos. Promoción de International Confidence Building Measures (CBM), protocolos conjuntos, La colaboración entre los sectores público y privado es esencial. Establecimiento de los estándares de seguridad en el sector industrial, Importa crear un procedimiento operativo estándar para una forma simplificada y adecuada de responder a un ataque cibernético. Nivel técnico y político". Stuxnet Group, "Modulo de Cybersecurity" (Powerpoint presentation, Modulo de Cybersecurity, Colégio Interamericano de Defesa, Washington, DC, 12 de março de 2018).

[66] Choucri and Goldsmith, "Lost in cyberspace", 76.

um subsídio para auxiliar na formação de uma consciência situacional. Todavia, creio que mais importante do que a criação de espaços que permitam o conhecimento das questões suscitadas neste artigo, seja a criação de espaços e oportunidades que promovam de forma efetiva o diálogo.

Este diálogo, precursor da construção de confiança (entre os países e atores integrantes do espaço cibernético), bem como da criação de alternativas construtivas, tem sido buscado e promovido de forma incansável pelo Colégio Interamericano de Defesa, não só por meio do Curso de Segurança Cibernética, mas também por meio da forma integrada com que essa disciplina é inserida dentro de um contexto coordenado com outras matérias como Política de Defesa, Segurança Multidimensional, Economia de Defesa e Pensamento Estratégico. Trata-se se um valor agregado intangível para as nações e para o hemisfério, que permitirá uma melhor preparação futura, proporcional os desafios que nos esperam.

Bibliografia

Abebe, Daniel. "Cyberwar, international politics, and institutional design". *University of Chicago Law Review* 83 n.1 (Winter, 2016): 1-22.

Agência Brasil. "Brasil é o 4º país em número de usuários de internet", *Exame*, acessado em 14 de junho de 2018. https://exame.abril.com.br/tecnologia/brasil-e-o-4o-pais-em-numero-de-usuarios-de-internet/.

Blum, Andrew. "Discover the physical side of the Internet". June 2012. TED Talk, 11:53. http://www.ted.com/talks/andrew_blum_what_is_the_internet_really

Cardoso Viana Gonçalves, Lívia. "Ensaio Reflexivo". Módulo de Economia de Defesa, Colegio Interamericano de Defesa, Washington, DC, janeiro de 2016.

———. "Fórum #2, Módulo Cybersecurity do Colégio Interamericano de Defesa". Moodle, 25 de fevereiro de 2018.

Caro Bejarano,Maria José. *La Protección de las infraestructuras criticas*. Madrid: Instituto Español de Estudios Estratégicos, 2011.

Center for Strategic and International Studies. "Cybersecurity Report 2016: Are We Ready in Latin America and the Caribbean?" March 2016. CSIS Events, 1:49:13. https://www.csis.org/events/cybersecurity-report-2016-are-we-ready-latin-america-and-caribbean.

Charney, Scott. "Collective defense: Applying the Public-Health Model to the Internet". *IEEE Security and Privacy* 10, n.2 (March-April, 2012): 54-59.

Choucri, Nazli and Daniel Goldsmith. "Lost in cyberspace: Harnessing the Internet, international relations and global security". *Bulletin of the Atomic Scientists* 68, n.2 (2012): 70 - 77. doi:10.1177/0096340212438696.

Collins, Sean and Steven McCombie. "Stuxnet: the emergence of a new cyber weapon and its implications". *Journal of Policing, Intelligence, and Counter Terrorism* 7, n. 1 (2012): 80-91.

https://www.tandfonline.com/doi/citedby/10.1080/18335330.2012.653198?scroll=top&needAccess=true.

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. "Defining Cybersecurity". *Technology Innovation Management Review* 4, no. 10 (October 2014): 13-21. https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

Diniz, Gustavo and Robert Muggah. *A Fine Balance: Mapping Cyber (In)Security in Latin America, Strategic Paper 2*. Rio de Janeiro: Igarapé Institute, June 2012. https://igarape.org.br/wp-content/uploads/2015/05/A-fine-balance_Mapping-cyber-insecurity-in-Latin-America.pdf.

Gustavo Diniz, Robert Muggah, and Misha Glenny. *Deconstructing Cyber Security in Brazil: Threats and Responses*. *Strategic Paper 11*. Rio de Janeiro: Igarapé Institute, December 2014. https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf.

Fojón Chamoro, Enrique e Ángel F. Sanz Villalba. *Ciberseguridad en España: una propuesta para su gestión*. Madrid: Real Instituto Elcano, 2010.

Franko, Patrice. *La Economía de la Defensa: Introducción*. Traduzido por o Colegio Interamericano de Defesa como *A Economia da Economia da Defesa: Introdução*. Waterville, ME: Colby College, 2000.

Fronfía Mesa, Antonio. *Sobre La Naturaleza y Alcance de la Economía de la Defensa*. Madrid: Instituto Español de Estudios Estratégicos, 2016. http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO79-2012_Naturaleza_Economia_Defensa_AFonfria.pdf.

Glenny, Misha. "A Weapon We Can´t Control". *New York Times*, junho 24, 2012. Acessado em 31 de março de 2018. http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html.

Goldstein, Guy-Philippe. "How Cyberattacks Threaten Real World Peace". Paris in January 2010. TEDxParis, 9:17. https://www.ted.com/talks/guy_philippe_goldstein_how_cyberattacks_threaten_real_world_peace.

Hunker, Jeffrey. *Cyber War and Cyber Power: Issues for NATO Doctrine*. No. 62. Rome: Research Division - NATO Defense College, 2010.

International Telecommunication Union. "Landmark Decisions from Guadalajara. Cybersecurity". Acessado 10 de junho de 2018. http://www.itu.int/net/itunews/issues/2010/09/20.aspx.

"Legislação". Governo do Brasil. Acessado 18 de junho de 2018. http://www4.planalto.gov.br/legislacao

Leiva, Eduardo A. "Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Vision Global a una Vision Local". *Revista Latinoamericana de Ingeniería de Software 3* no. 4: 161-176. http://revistas.unla.edu.ar/software/article/view/775/826.

Luiijf, Eric and Kim Besseling, and Patrick De Graaf. "Nineteen National Cyber Security Strategies". *International Journal of Critical Infrastructures* 9, no. 1 (January 1, 2013): 3–31. doi:10.1504/IJCIS.2013.051608.

Ministério da Defesa. *Doutrina Militar de Defesa Cibernética*. Brasília: Ministério da Defesa, 2014. https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.

———. *Política Cibernética de Defesa*. Brasília: Ministério da Defesa, 2014. http://idciber.eb.mil.br/images/documentos/doutrina/manual_pol_nac_def.pdf.

Moore, Tyler. "The Economics of Cybersecurity: Principles and Policy Options". *International Journal of Critical Infrastructure Protection* 3, no. 3–4 (December 2010): 103-117.

Newmeyer, Kevin P. "Cybersecurity do Colégio Interamericano de Defesa". Colegio Interamericana de Defesa, Washington, DC, 3 de março de 2018.

———. "Cybersecurity do Colégio Interamericano de Defesa". Colegio Interamericana de Defesa, Washington, DC, 5 de fevereiro de 2018.

———. "Elements of National Cybersecurity Strategy for Developing Nations". *National Cybersecurity Institute Journal* 1, no. 3 (2015): 9-19.

———. "Modulo de Cybersecurity". Powerpoint presentation, Modulo de Cybersecurity, Colégio Interamericano de Defesa, Washington, DC, 12 de fevereiro no curso de ano 2018.

———. *Report on Cybersecurity and Critical Infrastructure in the Latin American and Caribbean 2018*. Washington, DC: OAS, 2018. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/cipreport.pdf.

Organization of American States. *Declaration. Strengthening Cyber-Security in the Americas*. CICTE/DEC.1/12 rev. 1. Washington, DC: Member States of the Inter-American Committee Against Terrorism (CICTE), March 7, 2012. https://www.oas.org/en/sms/cicte/Documents/Declarations/DEC_1%20rev_1_DECLARATION_CICTE00749E04.pdf.

———. *Report on Cybersecurity and Critical Infrastructure in the Americas 2015*. Washington, DC: Organization of American States and Trend Micro, 2015.

Presidência da República. Casa Civil. *Diário Oficial da União – Seção 1*. Brasília: Imprensa Nacional, 9 de setembro de 2009. http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/200.

Sánchez Medero, Gema. "Ciberespacio y el Crimen Organizado. Los nuevos desafíos del siglo XXI". *Revista Enfoques: Ciencia Política y Administración Pública* 10, n.16 (2012): 71-87.

Stuxnet Group. "Modulo de Cybersecurity". Powerpoint presentation, Modulo de Cybersecurity, Colégio Interamericano de Defesa, Washington, DC, 12 de março de 2018.

Tossi, Alejandro Amigo. "Consideraciones sobre la ciberamenaza a la seguridad nacional". *Revista Política y Estrategia* 125 (2015): 83-96.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. Pub. L. No. 107-56. § 1016.