Nota introdutória
Geopolítica contemporânea e os desafios para a segurança e a defesa cibernéticas

Danielle Jacon Ayres Pinto | *Marcos Aurélio Guedes de Oliveira* | *Natália Diniz Schwether*

A geopolítica contemporânea é marcada por rápidas mudanças, e as principais delas que podemos destacar são os avanços tecnológicos e a crescente interconexão global. Nesse cenário, um dos desafios mais significativos é garantir um espaço cibernético seguro e estável para a sociedade e para o Estado. As ameaças cibernéticas não apenas afetam indivíduos e organizações, mas também têm implicações profundas para a segurança nacional e a estabilidade internacional. Assim, esse dossiê aqui desenvolvido tem por intuito explorar as interseções entre geopolítica, segurança cibernética e defesa cibernética, analisando os principais atores, tipos de ameaças, desafios e estratégias de mitigação.

O rápido desenvolvimento tecnológico em um mundo hiperconectado traz consequências pouco previsíveis e de grande impacto. De maneira que cada vez mais casos envolvendo o uso do poder cibernético em conflitos interestatais são registrados, seja para realizar campanhas de reconhecimento e informação, seja para otimizar ou comprometer sistemas operacionais militares e/ou civis de infraestruturas físicas e impactar de modo significativo a moral doméstica dos alvos atingidos – foi possível ver tal situação ocorrer de forma efetiva na guerra que a Rússia trava contra a Ucrânia. Outro impacto que a revolução nas tecnologias de informação e comunicação produziu traduziu-se nos graves problemas globais que têm desafiado a ordem legal e social dos Estados, ao ponto de redefinir os laços da comunicação humana e pôr em xeque a ordem democrática – as manipulações digitais no pleito do Brexit, nas eleições americanas de 2016 e nas eleições brasileiras de 2018 são um claro exemplo desse cenário ameaçador em crescimento.

Dessa forma, a relação tecnológica, cultural e de poder tem levado à construção de um novo sistema internacional que acelera a ascensão de potências emergentes e redefine as relações Norte-Sul. Todas as áreas da ciência, inclusive as humanidades, estão incorporando essa questão em suas preocupações. Mas é no estudo da política internacional que se sobressai o tema de maneira mais contundente. Os ganhadores nesse processo

 https://doi.org/10.23906/ri2024.82a01

serão aquelas nações que melhor entendam os sinais dessas transformações e procurem incorporar esse aprendizado ao seu processo decisório.

Todavia, como podemos identificar as principais potências na área digital e quais seriam seus maiores recursos?

Antes de desenvolvermos essa questão, vale entender que o espaço cibernético se tornou o quinto domínio da guerra e os Estados-Nação utilizam ataques cibernéticos como ferramentas de coerção, poder e influência. A espionagem cibernética, a sabotagem e as campanhas de desinformação são algumas das estratégias empregadas por países para alcançar objetivos geopolíticos, e tudo isso ocorre frente a uma incipiente governança global nessa seara que resiste a se desenvolver por força e vontade dos Estados no sistema internacional. Quanto menos regras, menos governança e maiores recursos, mais a esfera cibernética passa a ser o espaço onde tudo se pode fazer e pouco se pode limitar ou punir. Vejamos: quem foi culpabilizado pelos ataques com o Stuxnet? Quais reais punições sofreu a Cambridge Analytica por manipular dados no pleito do Brexit? Qual punição receberam os *hackers* «patriotas» russos por usar de forma desvirtuada os algoritmos das mídias sociais, em especial do Facebook, na eleição dos Estados Unidos em 2016? Nenhuma punição relevante que evitasse que esse cenário não só se repetisse, como, principalmente, passasse a fazer parte das estratégias de ação de diversos atores no sistema internacional para conseguirem satisfazer suas demandas de poder e influência. A reação muitas vezes foi punir indivíduos, fazer algum tipo de legislação interna e aumentar o investimento no desenvolvimento de tecnologia com fins securitários. Nenhuma outra ação ao nível global avançou no sentido de evitar ataques, pelo contrário, o que se viu foi o aumento do uso indiscriminado e descontrolado de meios digitais para ataques de todos os tipos e uma clara deterioração da segurança cibernética e da defesa cibernética no mundo.

Mas vejamos quem são os principais atores estatais que dominam as tecnologias cibernéticas no mundo.

Os Estados Unidos, que emergem como um dos principais atores na arena da segurança cibernética, investindo significativamente em infraestrutura cibernética e em capacidades ofensivas e defensivas. Agências como a National Security Agency e o Cyber Command desempenham papéis críticos na proteção de ativos nacionais e na condução de operações cibernéticas no exterior. A doutrina cibernética dos Estados Unidos enfatiza tanto a defesa quanto a dissuasão ativa.

A Rússia também é amplamente reconhecida por suas capacidades avançadas em ciberespionagem e ciberataques. Incidentes como o hackeamento do Comitê Nacional Democrata dos Estados Unidos em 2016 e os ataques à infraestrutura ucraniana demonstram a eficácia e a ambição das operações cibernéticas russas. A Rússia utiliza ciberoperações como extensão de suas estratégias de guerra híbrida, visando desestabilizar adversários e influenciar processos políticos.

A China é outro jogador chave, com extensas atividades de ciberespionagem econômica e militar. O país tem sido acusado de roubar propriedade intelectual e segredos industriais de empresas ocidentais, além de realizar operações de influência política. As capacidades cibernéticas da China são vistas como parte integrante de sua estratégia de modernização militar e de sua ambição de se tornar uma superpotência tecnológica. O Estado de Israel é amplamente reconhecido por suas capacidades cibernéticas avançadas e por ser um dos líderes mundiais em segurança cibernética. O país tem investido significativamente em tecnologia cibernética, tanto para fins defensivos quanto ofensivos. Unidades militares especializadas, como a Unidade 8200, são conhecidas por suas operações sofisticadas de ciberespionagem e guerra cibernética. Esse país também é um centro de inovação cibernética, com um ecossistema robusto de *startups* e empresas de tecnologia que desenvolvem soluções avançadas de segurança cibernética. A colaboração entre o setor militar, governo e indústria privada tem sido um fator chave no fortalecimento das capacidades cibernéticas de Israel.

Todavia, existem também outros países com menor capacidade, mas que já entenderam que os recursos cibernéticos são fulcrais para o novo embate geopolítico mundial. Estados como o Irã e a Coreia do Norte têm investido em capacidades cibernéticas para compensar suas desvantagens em termos de poder militar convencional. Além disso, grupos não estatais, como *hackers* independentes e organizações terroristas, representam ameaças adicionais. A proliferação de ferramentas cibernéticas acessíveis aumentou o risco de ataques provindos de diversos atores e por diversos motivos. Assim, o espaço cibernético é um espaço inseguro por essência, mas também, e muitas vezes, por escolha e necessidade dos Estados que mais controlam essas tecnologias.

Mas como mudar esse cenário e tornar o mundo digital mais seguro para cidadãos, empresas, organizações não governamentais e Estados?

Podemos pensar em algumas alternativas.

A primeira alternativa seria o incremento da cooperação internacional para combater ameaças cibernéticas. Todavia, como já dissemos acima, essa é dificultada por questões de soberania, confiança mútua e interesses divergentes. A criação de normas e padrões globais para a segurança cibernética é um desafio contínuo. Iniciativas como o Grupo de Peritos Governamentais da Organização das Nações Unidas sobre Avanços na Informação e na Tecnologia de Comunicação são passos importantes, mas a implementação e a adesão permanecem complexas.

Melhorias nas regulamentações e políticas nacionais na área são uma questão urgente. Desenvolver e implementar políticas eficazes de segurança cibernética é crucial e isso inclui legislações que exijam padrões de segurança para empresas e infraestrutura crítica, bem como estratégias nacionais de defesa cibernética. A regulação deve equilibrar a proteção contra ameaças e a promoção da inovação tecnológica.

Investir pesado em educação tecnológica e capacitação é a forma mais eficaz de fazer perdurar no tempo medidas de segurança e de defesa cibernéticas. A formação de

profissionais qualificados em segurança cibernética é vital. A demanda por especialistas excede a oferta, e há uma necessidade urgente de programas educacionais e de treinamento para preencher essa lacuna. Todavia, mais importante que formar profissionais especializados na área é dar ao cidadão comum, principalmente aos mais vulneráveis que são os idosos e as crianças, formação para utilizarem as tecnologias sem que se tornem presas fáceis para a criminalidade digital. Um processo efetivo de higiene cibernética, como o realizado no continente europeu, deveria ser um exemplo para o mundo todo de como agir nessa esfera.

Assim, a geopolítica contemporânea e a segurança cibernética estão indissociavelmente ligadas. Os desafios para a defesa cibernética são complexos e multifacetados, exigindo uma abordagem coordenada e inovadora. À medida que a tecnologia continua a evoluir, a importância da segurança cibernética na geopolítica global só tende a aumentar, tornando-se uma área crucial para a segurança nacional e a estabilidade internacional. A colaboração internacional, a inovação tecnológica, a educação e a formulação de políticas eficazes são essenciais para enfrentar os desafios presentes e futuros.

Para promover o debate nesse sentido, esse dossiê especial sobre «Geopolítica contemporânea e os desafios para a segurança e a defesa cibernéticas» vai trazer sete artigos que debaterão diferentes temas.

O artigo «Cooperação em segurança e defesa cibernética e a proteção das democracias sul-americanas», das autoras Jéssica Maria Grassi, Danielle Jacon Ayres Pinto e Graciela de Conti Pagliari, vai problematizar como a proteção das democracias na região sul-americana está intrinsecamente conectada com o aprimoramento do conceito de segurança e defesa cibernéticas.

No artigo seguinte, com o título «A cibernética na grande estratégia: um estudo comparado de Reino Unido, França e Portugal», a proposta dos autores Natália Diniz Schwether e Marcos Aurélio Guedes de Oliveira é promover uma comparação das grandes estratégias de países centrais na política internacional e perceber como esses documentos tratam a questão cibernética.

No terceiro artigo, com o título «Proteção de dados: experiência internacional e o caso brasileiro – relação com a segurança da informação e a governança cibernética», os autores Constança Maria Maia Arruda e Pedro Arthur Linhares Lima trazem um debate muito atual sobre como proteger os dados no ciberespaço e como criar uma governança para aprimorar esses processos.

No próximo artigo, intitulado «Defesa cibernética na guerra russo-ucraniana: um mapeamento dos ataques cibernéticos às infraestruturas críticas da Ucrânia», os autores Thays Felipe David de Oliveira, Renato Victor Lira Brito e Priscylla Cristina de Souza Lippo identificam os principais ataques cibernéticos russos às infraestruturas ucranianas, quais foram os principais alvos e o porquê da sua escolha.

No artigo seguinte, o tema tratado foi «Marco zero: as origens da guerra cibernética orquestrada pelos Estados Unidos da América para atingir a República Islâmica do Irã

(2007-2010)»; escrito pelos autores Fernando H. Casalunga, Eduardo Munhoz Svartman e Bruno Cardoso Reis, o artigo vai debater as estratégias de ataques cibernéticos dos Estados Unidos frente ao Irã e quais foram os ganhos auferidos nessa ação.

No sexto artigo, com o título «Ordem e progresso? Analisando as respostas brasileiras aos cibercrimes», os autores Mariana Grilli Belinotte, Luiz Rogério Franco Goldoni, Joe Devanny e Carlos Frederico Coelho debatem os avanços do Brasil na resposta normativa e prática aos crimes cibernéticos que a sociedade desse país vem enfrentando.

No sétimo artigo, com o título «Consciência situacional como ferramenta estratégica da defesa cibernética», os autores André Lucas Alcântara da Silva e Gills Vilar-Lopes promovem o debate da importância da consciência situacional para promoção da defesa cibernética dos Estados frente às novas ameaças que enfrentam atualmente.

Por fim, esperamos que os artigos desenvolvidos nesse dossiê possam servir de base para aprimorar o debate em torno do tema e produzir processos securitários mais efetivos e que busquem a segurança da sociedade, do indivíduo, dos atores privados e do Estado de forma efetiva e numa lógica colaborativa e nunca belicosa. R:I

Danielle Jacon Ayres Pinto Investigadora sénior do Núcleo de Pesquisa em Política Internacional, Segurança e Defesa (NPSeD). Doutora em Ciência Política pela Universidade Estadual de Campinas (UNICAMP). Professora no Curso de Relações Internacionais e coordenadora do Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina (UFSC). > Centro Socioeconômico – CSE UFSC, R. Roberto Sampaio Gonzaga-Trindade, Florianópolis, Brasil | danielle.ayres@ufsc.br

Marcos Aurélio Guedes de Oliveira Professor titular do Departamento de Ciência Política da Universidade Federal de Pernambuco. > Centro de Filosofia e Ciências Humanas (CFCH) – UFPE, Rua Acadêmico Hélio Ramos, s/n, 6.º andar, Cidade Universitária – Recife, PE, Brasil | marcosaurelioguedes@gmail.com

Natália Diniz Schwether Doutora e pós-doutora em Ciência Política pela Universidade Federal de Pernambuco. > Centro de Filosofia e Ciências Humanas (CFCH) – UFPE, Rua Acadêmico Hélio Ramos, s/n, 6.º andar, Cidade Universitária – Recife, PE, Brasil | n.schwether@unesp.br