A SECURITIZAÇÃO DO "QUINTO DOMÍNIO": OS ATAQUES CIBERNÉTICOS DA ESTÔNIA (2007) E SEUS IMPACTOS NA POLÍTICA INTERNACIONAL

Maria Eduarda de Paiva Pereira[1]
Gabriel Fernandes Caetano[2]

RESUMO

O presente trabalho aprofunda a análise da securitização do ciberespaço como um "novo domínio" da segurança, através dos ataques cibernéticos à Estônia (2007) e da influência causada na política internacional. A partir da análise do contexto que levou aos ataques, o estudo busca entender o impacto das vulnerabilidades críticas na defesa cibernética, o estímulo a discussões acerca da criminalidade cibernética e o reconhecimento de uma área estratégica em ascensão. Com base no conceito de securitização da Escola de Copenhague, analisam-se as respostas político-institucionais adotadas por Estados e instituições internacionais no cenário pós-ataque, bem como o enquadramento das ameaças no ciberespaço como um risco à segurança global. Observa-se uma mudança significativa na percepção de segurança, assim como as medidas foram essenciais na mitigação e consolidação de uma governança digital voltada à cooperação, proteção e fortalecimento da segurança cibernética. Conclui-se, portanto, que os ataques à Estônia atuaram como um catalisador na construção da estabilidade no ciberespaço.

Palavras-chave: securitização; ciberespaço; Estônia; ataque cibernético; defesa cibernética.

[1] Graduanda do curso de Relações Internacionais pelo Centro Universitário IESB.
[2] Mestre em Relações Internacionais pela Universidade Estadual da Paraíba e professor do curso de Relações Internacionais no Centro Universitário IESB.

Abstract

This paper delves into the analysis of cyberspace securitization as a "new domain" of security, using the 2007 cyberattacks on Estonia and their influence on international policy as a case study. By examining the context that led to these attacks, the study aims to understand the impact of critical vulnerabilities on cyber defence and the encouragement of discussions on cybercrime, as well as the recognition of cyberspace as an emerging strategic area. Based on the Copenhagen School's securitization concept, the paper analyzes the political-institutional responses adopted by states and international institutions in the post-attack scenario, as well as the framing of cyber threats as global security risks. A significant shift in security perception is observed, and the measures taken were essential for mitigating risks and establishing digital governance focused on cooperation, protection, and strengthening of cybersecurity. It is concluded that the attacks on Estonia acted as a catalyst for building stability in cyberspace.

Keywords: securitization, cyberspace; Estonia; cyberattack; cyber defence.

1. Introdução

O ciberespaço emerge como o mais recente campo de disputa na política internacional. Reconhecido como o "quinto domínio", ele se une aos clássicos campos geopolíticos — terra, mar, ar e espaço — ampliando a arena de conflitos contemporâneos e desafiando estruturas tradicionais de segurança (The Economist, 2010). Guerras cibernéticas são, como afirmam Paulo Shakarian, Jana Shakarian e Andrew Ruef (2017), uma extensão da política por ações realizadas no ciberespaço por atores estatais ou não estatais que constituem uma ameaça séria à segurança de uma nação ou são realizadas em resposta a uma ameaça percebida contra a segurança de uma nação.

Em abril de 2007, a Estônia foi alvo de uma série de ataques cibernéticos desencadeados por interesses políticos russos. Esses ataques foram um marco na segurança cibernética e preocupação dos atores internacionais – estatais e não estatais -, devido à grande vulnerabilidade dos aspectos públicos do país serem integrados à internet (Haataja, 2017).

Tendo em vista a importância fundamental dos impactos que os ataques cibernéticos influenciaram o sistema internacional enquanto ferramenta para a segurança cibernética, em um discurso à Assembleia Geral das Nações Unidas (ONU), em setembro de 2007, o Presidente da Estônia declarou que:

> "Os ataques cibernéticos são uma ameaça não apenas para sistemas de tecnologia da informação sofisticados, mas também para a comunidade como um todo. Por exemplo, eles poderiam ser usados para paralisar os serviços médicos de emergência de uma cidade. As ameaças da guerra cibernética têm sido frequentemente subestimadas, pois, felizmente, ainda não resultaram na perda de vidas humanas. … Além de medidas técnicas e legais concretas para combater os ataques cibernéticos, os governos precisam definir moralmente a violência e o crime cibernéticos, que merecem ser condenados da mesma forma que o terrorismo ou o tráfico de seres humanos. Combater a guerra cibernética é do interesse de todos nós, sem exceção."[3]

Desse modo, o presente artigo busca responder aos seguintes questionamentos: Como o ataque cibernético da Estônia (2007) influenciou os debates e tomadas de decisão sobre crimes cibernéticos globalmente? Como países e organizações internacionais enquadraram a questão cibernética como ameaça? Quais medidas de interesse coletivo foram criadas para lidar com os crimes cibernéticos?

Nesse sentido, o objetivo geral deste trabalho é compreender a relação entre criminalidade cibernética e segurança internacional. Pretende-se, portanto, explorar as medidas adotadas por países e organizações internacionais no contexto pós-Estônia, focando no enquadramento da questão enquanto ameaça, bem como nas estratégias construídas para mitigá-las.

O presente artigo terá como perspectiva teórica-conceitual o conceito de *securitização*, da Escola de Copenhague. A teoria explora como questões políticas ou sociais são elevadas ao grau de ameaças existenciais, legalizando medidas extraordinárias para lidar com elas. No contexto cibernético, o ciberespaço é enxergado como o domínio onde as ameaças podem surgir e ser securitizadas por Estados e organizações internacionais. Ataques cibernéticos ou vulnerabilidades digitais são ameaças que podem surgir à soberania estatal. Aplicando o pensamento da Escola de Copenhague, observaremos como questões dentro da segurança cibernética são ameaças securitárias que exigem ações e respostas imediatas.

Para tanto, este estudo orienta-se por uma abordagem metodologicamente qualitativa, baseada na exploração e interpretação de fontes primárias e secundárias relacionadas à guerra cibernética no âmbito internacional. Serão abordados documentos oficiais publicados por organizações internacionais, como a OTAN e União Europeia, bem como discursos oficiais. As

[3] "Cyber attacks are a threat not only to sophisticated information technological systems, but also to a community as a whole. For instance,they could be used to paralyse a city's emergency medical services. The threats posed by cyber warfare have often been underestimated since, fortunately, they have so far not resulted in the loss of any lives.… In addition to concrete technical and legal measures for countering cyber attacks, governments must morally define the cyber violence and crime, which deserve to be generally condemned just like terrorism or the trafficking in human beings.Fighting against cyber warfare is in the interests of us all without exception" (ILVES, 2007, tradução própria).

fontes secundárias incluirão uma ampla revisão bibliográfica da produção acadêmica sobre guerras cibernéticas e segurança internacional.

Nesse sentido, além desta introdução, o artigo está dividido em três partes: na primeira parte, será apresentado todo o contexto histórico dos eventos que levaram aos ataques, abrangendo a sequência temporal e as principais táticas utilizadas. A segunda parte, por sua vez, apresentará as respostas, medidas de mitigação e de recuperação da Estônia e a criação de novas políticas de segurança. Por último, a terceira parte analisará como a comunidade internacional respondeu aos ataques, incluindo iniciativas de apoio à Estônia e ações preventivas a futuros ataques, assim como, o surgimento da discussão sobre as normas internacionais de segurança cibernética e acordos internacionais multilaterais.

2. A Escola de Copenhague e a securitização

Os Estudos de Segurança Internacional (ESI), uma das subáreas das Relações Internacionais (RI), desenvolveu-se rapidamente no pós-Segunda Guerra Mundial, focando inicialmente na proteção do Estado contra ameaças externas e internas (Buzan & Hansen, 2012). Os ESI possuem três grandes fases que marcaram sua evolução: a primeira fase começa a partir do final dos anos 1940, com o Estado como principal objeto de referência. Com a proteção estatal assegurada, era possível proteger outros objetos de referência e garantir a "segurança nacional". Na segunda fase, a vertente tradicionalista dos ESI passam a ser desafiados por novas perspectivas como, por exemplo, os *peace studies* e os movimentos por desarmamento. Na terceira fase, marcada a partir da década de 1980, observa-se a ampliação e o aprofundamento da agenda de segurança. Para além do estadocentrismo e das ameaças militares, outros setores passam a compor a agenda dos ESI. Identificam-se, por exemplo, ameaças econômicas, ambientais e societais que não estavam limitadas à lógica bipolar nem reduzidas as preocupações nucleares (Buzan & Hansen, 2012).

Como citado, a partir da Pós-Guerra Fria, os conceitos passam por transformações. A agenda fortemente militar no início começa a ser ampliada para temas além do enfoque político-militar. A disciplina divide-se em diversas abordagens, como os estudos feministas de segurança, estudos críticos de segurança e a escola de Copenhague, considerando abordagens mais diversificadas (Buzan e Hansen). "Segurança" deixa de ser até então um conceito concreto da perspectiva militarista e tradicional e transita para questões atuais como segurança econômica, ambiental, societal e cibernética. Nessa evolução, surgem várias escolas de

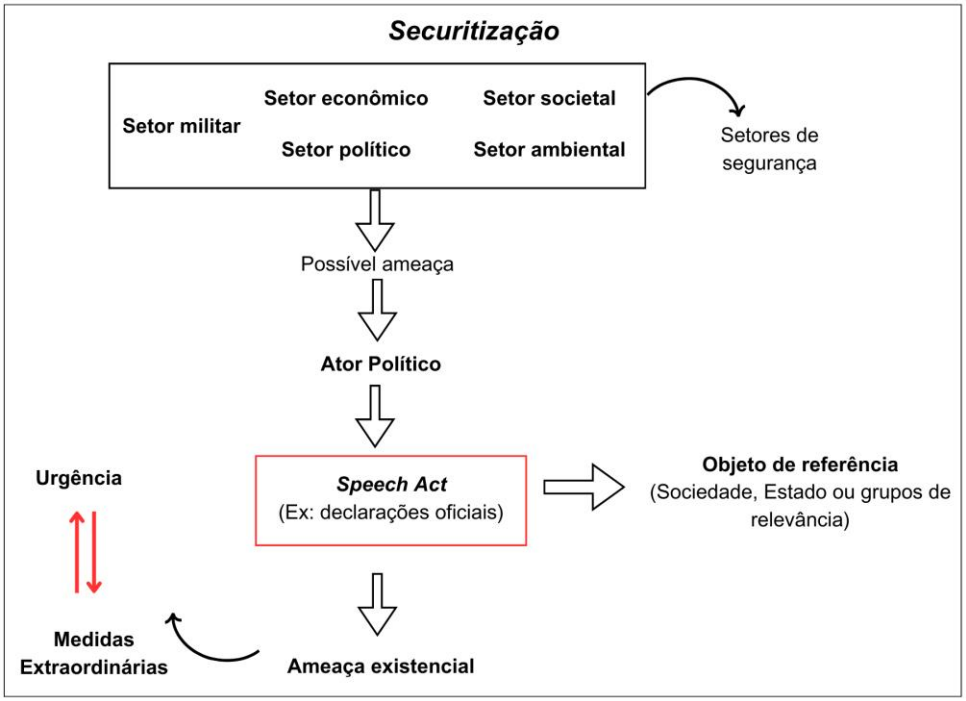
pensamento que abordam os ESI, como a Escola Galesa de Estudos Críticos de Segurança, a Escola de Copenhague e a Escola de Paris.

O *Copenhagen Peace Research Institute* (COPRI), mais conhecido como Escola de Copenhague, foi fundado em 1985, tendo como finalidade a promoção dos estudos para a paz (Rolf, 2022). Desde a sua formação, é referência pela contribuição da teoria da securitização, que deixa de lado a tradicional visão[4] de segurança já mencionada e adota uma abordagem mais discursiva, ancorada nos atos de fala (Buzan, Wæver & Wilde, 1998). Segundo Waever (1995), a securitização é um ato de fala (*speech act*) onde um ator político declara algo como ameaça existencial, transformando o assunto em uma questão de segurança a um objeto referencial (geralmente sociedade, Estado ou grupos de maior relevância). Com isso, medidas extraordinárias podem ser justificadas. Qualquer assunto pode ser securitizado, desde que haja um convencimento da audiência de que se trata de uma questão urgente e uma ameaça existencial a um objeto de referência. Buzan e Hansen argumentam que a securitização pode acontecer em vários setores.

Com essa ampliação do conceito de segurança, Buzan, Wæver e Wilde (1998) apresentam outros setores nos quais pode ocorrer a securitização, tal como sintetizado na figura 1 abaixo: no setor militar, que é a tradicional defesa da integridade do Estado; no setor político, e a ameaça pode desestabilizar instituições de governança; no setor econômico, há uma preocupação com o risco dos sistemas financeiros colapsarem e perderem as suas autonomias econômicas; no setor societal, o qual está relacionado com a identidade coletiva, seja étnica ou religiosa; e no setor ambiental, apresentando riscos para a sociedade através de ameaças como desastres ambientais ou mudanças climáticas.

[4] Para uma visão crítica sobre o conceito de securitização e a Escola de Copenhague ver: Williams (2003).

Figura 1 - Quadro síntese processo de securitização



Fonte: Elaborado pela autora com base em Buzan, Wæver & Wilde (1998)

Entretanto, securitizar não é apenas reconhecer a ameaça iminente; trata-se de utilizar o potencial perigo para legitimar medidas extraordinárias. Segurança é um processo discursivo, ou seja, é construído por meio da linguagem e da compreensão (Wæver, 1995). Portanto, não é um estado concreto, mas um conceito capaz de transformar qualquer assunto em uma questão de sobrevivência.

Ao enfatizar diferentes temas como um problema de segurança, a teoria demonstra a sua flexibilidade e permite uma reflexão crítica do que pode ou não ser securitizado. Por isso, será aplicado o conceito da vertente da Escola de Copenhague no campo da segurança cibernética. Utilizando como exemplo os discursos que enquadram os ataques cibernéticos como uma ameaça existencial a partir da criação de uma lógica de urgência.

2.1 Segurança cibernética e o conceito de securitização

No contexto da segurança cibernética, o ciberespaço, entendido como um novo campo para a proliferação de ameaças, é definido pelo Departamento de Defesa dos Estados Unidos

(2010, p. 58) como: “um domínio global dentro do ambiente de informação, composto pela rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas de computadores e processadores e controladores embarcados”[5].

De acordo com o *The Economist* (2010) “o ciberespaço é agora considerado o quinto domínio de guerra, após terra, mar, ar e espaço”[6]. Hansen e Nissenbaum (2011) relacionam três pontos que fazem a cibersegurança se encaixar no processo de securitização: (i) os ataques cibernéticos são a ameaça existencial, capazes de colapsar sistemas essenciais e gerar crises, sejam elas econômicas, políticas ou sociais; (ii) ciberataques são uma ameaça direta às infraestruturas críticas, serviços sociais e informação de dados pessoais; e (iii) o objeto de referência pode ser o Estado, mas abrange também indivíduos e atores estatais e não estatais pelas complexidades da ameaça existencial. Logo, o quadro permite a adoção de políticas de defesa ou controle digital que são normalmente intrusivas, ou fazem uso das forças militares cibernéticas para combater os ataques cibernéticos. Assim justificam-se as medidas extraordinárias para securitizar o ciberespaço.

A partir do ponto abordado, o que acontece no ciberespaço e a securitização estão relacionados. Lene Hansen e Helen Nissenbaum (2011) apresentam novos conceitos dentro da segurança cibernética que auxiliam no entendimento deste artigo e como o processo funciona na prática. É necessário compreender que, ao securitizar, existe uma “tecnificação”. O ciberespaço é uma questão técnica, pois a cibersegurança é um problema técnico que exige uma abordagem especializada por profissionais de tecnologia da informação. Por ser uma abordagem especializada, muitas vezes se torna despolitizada e passa uma imagem de neutralidade, o que, segundo Hansen e Nissenbaum (2011) pode mascarar implicações políticas incômodas.

Atualmente, utilizamos a Internet para tudo em nosso dia a dia, seja para realizar pagamentos, fazer compras ou conhecer novas pessoas. Com “práticas cotidianas de segurança”, podemos securitizar ameaças comuns, como violação de privacidade, fraude digital ou roubo de identidade. Nesse contexto, a securitização passa a fazer parte da rotina e é essencial na proteção das atividades diárias em uma sociedade cognitivamente *on-line* (Hansen e Nissenbaum, 2011).

---

[5] “A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers”(DEPARTMENT OF DEFENSE, 2010, tradução própria) .

[6] “After land, sea, air and space, warfare has entered the fifth domain: cyberspace”(THE ECONOMIST, 2010, tradução própria).

Existe a possibilidade de cenários catastróficos de desastres acontecerem em larga escala, como aconteceu na Estônia, onde um ataque cibernético pode desencadear falhas de segurança em cascata, afetando a segurança nacional. A "hipersecuritização" não apenas identifica a ameaça como urgente, mas a dramatiza, de modo que o Estado responda a curto prazo, muitas vezes alimentando o entendimento público do perigo iminente. Caso não houvesse essa "hipersecuritização", as medidas extraordinárias poderiam ser consideradas desnecessárias ou excessivas (Hansen e Nissenbaum, 2011).

A securitização da Escola de Copenhague, em conjunto com a segurança cibernética, possui uma estrutura rica em informações no compreendimento de respostas às ameaças digitais. A flexibilidade da teoria, ao abordar questões emergentes, aponta até onde vão os limites tradicionais da segurança. Portanto pode-se observar, a partir do caso estoniano, a teoria aplicada na prática. Considerado o "primeiro ato de guerra cibernética", os ataques cibernéticos à Estônia afetaram não somente as infraestruturas críticas, como também outros setores de serviços sociais, gerando uma grande crise nacional e dúvidas na população em relação à proteção do território estoniano.

Nesse contexto, analisaremos, passando por toda a sequência temporal, os fatos que levaram a esse fatídico caso, como o Estado continua sendo o principal ator securitizador, além das respostas tomadas pela Estônia de maneira a conseguir securitizar o seu ciberespaço eficientemente após os ataques, tanto no âmbito nacional, quanto no âmbito internacional.

3. Estônia, *speech act* e a securitização dos ataques cibernéticos

A Estônia era reconhecida como um país pioneiro na digitalização, com sistemas avançados que permitiam aos cidadãos votar em eleições e acessar serviços bancários e públicos através da *e-Estonia*, "uma iniciativa do governo da Estônia para melhorar as interações dos cidadãos com o Estado, por meio do uso de soluções eletrônicas"[7] (Blue Ocean Strategy, 2024). Contudo, os ataques cibernéticos em 2007 expuseram o quanto a Estônia dependia da tecnologia e estava despreparada para defender seus sistemas. Não existiam medidas de proteção adequadas para a infraestrutura utilizada. Essa combinação demonstrou que a digitalização sem segurança tornou os ataques ainda mais devastadores e destacou a necessidade de investir em segurança cibernética na era digital.

[7] "A movement by the government of Estonia to improve citizen interactions with the state through the use of electronic solutions" (Blue Ocean Strategy, 2024, tradução própria)

No dia 26 de abril de 2007, o governo estoniano decidiu realocar a estátua do Soldado de Bronze de Tallinn de um parque na cidade para um cemitério militar. “O memorial foi erguido em 1947 para comemorar a vitória do Exército Soviético sobre a Alemanha Nazista na Segunda Guerra Mundial”[8] (“CYBERDEFENSE REPORT Estonia’s National Cybersecurity and Cyberdefense Posture Policy and Organizations”, [s.d.], p. 5). No entanto, essa mudança causou descontentamento, tanto dos próprios russos quanto dos russos étnicos que vivem na Estônia, devido ao forte simbolismo da estátua. Para os estonianos, a estátua representava a opressão russa durante o regime da URSS (GAMERO-GARRIDO, 2014).

Na manhã do dia seguinte, os ataques cibernéticos começaram. Foram três semanas enfrentando ataques sem precedentes, diretamente lançados contra o governo, as forças de segurança, o setor bancário, a mídia e a infraestrutura de internet (GEERS, [s.d.]). Embora o ataque tenha sido sem precedentes, uma vez que era possível identificar ataques de várias partes do mundo, muitos deles originaram-se de servidores russos. As autoridades estonianas atribuíram à Rússia a autoria dos ataques, enquanto o governo russo negou qualquer envolvimento oficial. Apesar das negativas, a Estônia chegou a acionar a OTAN, solicitando a aplicação do Artigo Quinto do Tratado do Atlântico Norte, que diz que “As Partes concordam que um ataque armado contra uma ou mais delas na Europa ou na América do Norte será considerado um ataque contra todas…”[9] (NATO, 2023). No entanto, os ataques cibernéticos não se configuraram como "ataques armados", resultando no indeferimento do pedido.

Como visto anteriormente, para securitizar, é necessário que os atores políticos apresentem atos de fala (*speech act*) para a população aprovar as medidas extraordinárias. Em maio de 2007, o Primeiro-Ministro estoniano Andrus Ansip declarou ao parlamento que:

> “…Isso, juntamente com os contínuos ataques cibernéticos originados de servidores de autoridades estatais russas, com o ato de arrancar a bandeira da Estônia de nossa embaixada e com as declarações dos delegados da Duma Russa, que pedem a mudança de governo na Estônia, indica que nosso estado soberano está sob um pesado ataque.Todos esses eventos evidenciam que não estamos lidando com assuntos internos, mas com uma intervenção bem coordenada e flagrante nos assuntos internos da Estônia. Nós recorremos à União Europeia e pedimos que tomem ações imediatas. Atacar um Estado-membro significa um ataque contra toda a União Europeia.”[10]

[8] “The memorial had been erected in 1947 to commemorate the victory of the Soviet Army over Nazi Germany in WWII.” (“CYBERDEFENSE REPORT Estonia’s National Cybersecurity and Cyberdefense Posture Policy and Organizations”, [s.d.], p. 5, tradução própria)

[9] “The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all…” (NATO, 2023, tradução própria)

[10] “...This, together with the continuing cyber-attacks from the servers of Russian state authorities, together with tearing the Estonian flag off our embassy and together with statements made by the delegates of the Russian Duma, calling for the change of government in Estonia, indicates that our sovereign state is under a heavy attack. All these events evidence that these are not our internal matters we are dealing with but it is a well-coordinated and

O discurso feito pelo Primeiro-Ministro exemplifica o conceito de "hipersecuritização" apresentada por Hansen e Nissenbaum (2011). Ansip estende as ameaças à segurança nacional para além das fronteiras locais e envolvendo a União Europeia, passa a enquadrá-las como uma questão de segurança supranacional. Nesse caso, há uma "dramatização" dos ataques cibernéticos e os outros atos para que ocorra uma mobilização e o apoio da UE em tomar respostas imediatas, legitimando medidas extraordinárias, mas também reforçando a segurança coletiva entre os Estados-membros e o senso de solidariedade. Outro exemplo importante de *speech act* é o discurso do Secretário-Geral da OTAN, Jaap de Hoop Scheffer, em setembro de 2007:

> "A Estônia montou uma defesa firme e habilidosa de sua infraestrutura de TI e conseguiu resistir ao ataque. Não tenho certeza se todos os países da OTAN conseguiriam se defender tão bem. Ataques cibernéticos podem derrubar uma rede elétrica, um sistema bancário e serviços governamentais. Embora os ataques ocorram no ciberespaço, seus efeitos são muito reais. E, embora não sejam militares no sentido tradicional, eles possuem uma clara dimensão de segurança, além de estarem ligados ao seu impacto econômico.... A OTAN também se transformou fundamentalmente para enfrentar esses novos desafios de segurança. Ao entrar neste novo século, tínhamos uma base sólida: membros que incluíam alguns dos países mais influentes do mundo; meio século de compromisso com a defesa mútua; um fórum de consulta política 24/7 entre Europa e América do Norte sobre questões de segurança; e uma capacidade incomparável de gerar poder militar. Construímos sobre essa base: antes de tudo, reconhecendo que a defesa estática já não é defesa alguma. É claro que reforçar a segurança interna é essencial: serviços de inteligência, polícia, monitoramento de fronteiras, câmeras de segurança. Mas, às vezes, também precisamos ir até o problema antes que ele chegue até nós."[11]

flagrant intervention with the internal affairs of Estonia.We have turned to the European Union and we ask them to take immediate action. Attacking one member state means an attack against the entire European Union"("Prime Minister Andrus Ansip's speech in Riigikogu", 2024, tradução própria).

[11] "Estonia put up a stout and skilled defence of its IT infrastructure, and weathered the storm. I'm not sure every NATO country could defend itself so well.Cyber attacks can take out a power grid, a banking system, and government services. While the attacks take place in cyber-space, the effects are very real. And while they are not military in the traditional sense, they have a clear security dimension, along with -- and linked to - -their economic impact…NATO, too, has transformed fundamentally to meet these new security challenges. Going into this new century, we had a rock-solid foundation: members that included some of the most influential countries in the world; half a century of commitment to one another's defence; a forum for 24/7 political consultation between Europe and North America on security matters; and an unmatched ability to generate military power. We have built on that foundation: first and foremost, by recognizing that static defence is no defence at all anymore. Of course, beefing up homeland security is essential: intelligence services, police, border monitoring, security cameras. But we also need sometimes to go to the problem before it comes to us."("NATO Speech: 'Today's NATO, and why it matters' - Speech by NATO Secretary General, Jaap de Hoop Scheffer, Lloyd's City Dinner, London, 5 September 2007", 2024, tradução própria).

No contexto do ciberespaço, utiliza-se de times de defesa da infraestrutura de TI, como feito pela Estônia na fala do Secretário-Geral, que demonstra o conceito de "tecnificação" ao proteger serviços essenciais pela abordagem especializada dos profissionais de tecnologia. Além disso, é notória a narrativa de medidas de monitoramento contínuo e prevenção proativa, a partir de práticas cotidianas de segurança, para que seja possível antecipar a ameaça antes que se torne um problema em escalada. Dessa forma, a OTAN usa como exemplo os ataques na Estônia para justificar medidas extraordinárias e se adaptar ao enfrentar novos desafios.

Vale ressaltar como um exemplo clássico da securitização o ato de fala proferido pelo Presidente estoniano, Toomas Hendrik Ilves, à Assembleia Geral das Nações Unidas (ONU), em setembro de 2007:

> "Os ataques cibernéticos são uma ameaça não apenas para sistemas de tecnologia da informação sofisticados, mas também para a comunidade como um todo. Por exemplo, eles poderiam ser usados para paralisar os serviços médicos de emergência de uma cidade. As ameaças da guerra cibernética têm sido frequentemente subestimadas, pois, felizmente, ainda não resultaram na perda de vidas humanas. … Além de medidas técnicas e legais concretas para combater os ataques cibernéticos, os governos precisam definir moralmente a violência e o crime cibernéticos, que merecem ser condenados da mesma forma que o terrorismo ou o tráfico de seres humanos. Combater a guerra cibernética é do interesse de todos nós, sem exceção."[12]

O presidente, por meio dessa fala, transforma os ataques cibernéticos em uma ameaça existencial que demanda uma resposta clara e imediata, envolve a comunidade internacional e requer ações de combate. Posto isso, há uma construção de um perigo com consequências graves que impacta diretamente a população. Ao comparar a "violência e os crimes cibernéticos" com ameaças abertamente condenadas, como tráfico humano e terrorismo, Toomas Ilves tenta elevar as guerras cibernéticas ao patamar dessas outras ameaças, para que medidas moralmente cabíveis sejam tomadas.

Portanto, essas falas, vistas por atores políticos, são estratégias discursivas que — corroboram a necessidade de se combater guerras cibernéticas por ser um interesse global — estimulam a aceitação pública sobre a segurança cibernética ser essencial e que devem ser aplicadas práticas para a mitigação desses riscos.

---

[12] "Cyber attacks are a threat not only to sophisticated information technological systems, but also to a community as a whole. For instance,they could be used to paralyse a city's emergency medical services. The threats posed by cyber warfare have often been underestimated since, fortunately, they have so far not resulted in the loss of any lives.… In addition to concrete technical and legal measures for countering cyber attacks, governments must morally define the cyber violence and crime, which deserve to be generally condemned just like terrorism or the trafficking in human beings.Fighting against cyber warfare is in the interests of us all without exception" (ILVES, 2007, tradução nossa).

4. Respostas político-institucionais no contexto pós-Estônia

Após os ataques cibernéticos, uma série de medidas e ações foram adotadas pela Estônia, por organizações internacionais e instituições, como respostas político-institucionais no enfrentamento e mitigação de ameaças cibernéticas na esfera global. Essas respostas abrangem desde a criação de centros de defesa especializados, como o Centro de Excelência de Defesa Cibernética Cooperativa da OTAN (CCDCOE), políticas nacionais de segurança e a formulação de normas e estratégias como a Diretiva NIS da União Europeia. Essas iniciativas têm por objetivo buscar o fortalecimento da resiliência digital, definir diretrizes seguras dentro do ciberespaço e promover a colaboração entre países, respondendo à crescente necessidade securitizar e estabilizar o ambiente digital.

A Estônia trabalhou ativamente na formulação dessas respostas; uma das principais medidas adotadas foi a primeira **Estratégia Nacional de Segurança Cibernética**, desenvolvida em 2008. A estratégia tinha por objetivo implementar e desenvolver padrões de segurança, aperfeiçoar o quadro jurídico, melhorar as habilidades, elevar a conscientização sobre a cibersegurança e estimular a cooperação internacional ("CYBERDEFENSE REPORT Estonia's National Cybersecurity and Cyberdefense Posture Policy and Organizations", [s.d.]). Além disso, o Ministério da Defesa, juntamente com a comunidade de cibersegurança estoniana, aceitou a proposta de consolidar uma **Liga de Defesa Cibernética** nos modelos da já existente Liga de Defesa da Estônia. A partir disso, por meio de um ato legal, foram criadas as Unidades de Defesa Cibernética (CDU), que são uma forma de colaboração nacional voluntária integrada à Liga de Defesa Estoniana (PERNIK; TUOHY, 2013). "A unidade busca proteger o estilo de vida de alta tecnologia da Estônia, protegendo a infraestrutura de informação e apoiando os objetivos mais amplos da defesa nacional."[13] (KASKA; OSULA; STINISSEN, 2013).

É notório o quanto a Estônia firma parcerias com outros Estados e organizações internacionais no compartilhamento de informações e práticas de tecnologias relacionadas ao fomento da segurança cibernética. O maior exemplo, é a colaboração com a OTAN na criação do **Centro de Excelência de Defesa Cibernética Cooperativa (CCDCOE)**. O centro, criado em 2008 e sediado em Tallinn, é uma iniciativa essencial na área de cooperação em defesa

[13] "The unit seeks to protect Estonia's high-tech way of life by protecting information infrastructure and supporting the broader objectives of national defence" (KASKA; OSULA; STINISSEN, 2013, tradução própria).

cibernética e uma grande referência nos estudos e estratégias de defesa digital. “A organização militar internacional concentra-se em pesquisas e desenvolvimento aplicados de maneira interdisciplinar, além de oferecer consultorias, treinamentos e exercícios no campo da cibersegurança”[14] (“NATO Cooperative Cyber Defence Centre of Excellence”, [s.d.]). O exercício ***Locked Shields***, organizado pelo CCDCOE, é o mais complexo exercício internacional de defesa cibernética com ataques em tempo real. É considerado uma oportunidade única para as nações fortalecerem seus sistemas sob forte pressão de ataques cibernéticos, a partir dos exercícios (“NATO Cooperative Cyber Defence Centre of Excellence”, [s.d.]).

Vale ressaltar que o Manual de Tallinn, apesar de não ser uma resposta político-institucional no sentido tradicional — justamente por não ter sido elaborado pelo governo ou organização internacional com autoridade legislativa — oferece orientações jurídicas na aplicabilidade do direito internacional em conflitos cibernéticos. Trata-se de uma iniciativa acadêmica e “neutra” em relação a políticas e questões políticas, não representando a posição jurídica ou doutrina de qualquer Estado ou organização internacional, incluindo o CCDCOE (CCDCOE, 2017).

Entretanto, o CCDCOE não foi a única resposta político-institucional da OTAN. Em 2016, na Cúpula da OTAN, os países alinhados reconheceram o ciberespaço como um novo domínio operacional o qual a OTAN deve ser capaz de defender (NATO, 2024). Essa decisão concedeu à aliança o desenvolvimento de políticas adequadas para o ciberespaço, além de possibilitar um gerenciamento mais efetivo entre os membros na resposta aos ataques cibernéticos. A Política de Defesa Cibernética da OTAN, criada em 2014 e atualizada em 2017, trouxe mudanças importantes. Baseado na Política, é tarefa central de defesa coletiva da OTAN a defesa cibernética. O Artigo 5 do Tratado do Atlântico Norte, anteriormente citado pela Estônia e indeferido por não ser considerado um ataque armado, atualmente pode ser invocado em caso de ataques cibernéticos com efeitos análogos ao de um ataque cibernético convencional. Além disso, tem por objetivo reforçar a cooperação com a União Europeia e outros parceiros internacionais na questão cibernética, por meio de treinamentos, compartilhamento de informações e orientações (“CCDCOE”, 2014).

A União Europeia (UE) foi uma das organizações que mais adotou respostas no fortalecimento da segurança cibernética de seus Estados-Membros no cenário europeu. Em

[14] “The international military organisation focuses on interdisciplinary applied research and development, as well as consultations, trainings and exercises in the field of cyber security”(“NATO Cooperative Cyber Defence Centre of Excellence”, [s.d.]).

2016, a UE implementou a **Diretiva de Segurança de Redes e Informação (Diretiva NIS)**, com base no Artigo 114 do Tratado sobre o Funcionamento da União Europeia, que visa aperfeiçoar, dentro de um nível padrão comum de segurança, os sistemas de rede dentro do bloco, impondo medidas mais rigorosas e exigindo a notificação de incidentes relevantes às autoridades nacionais de cibersegurança ("BRIEFING Implementation Appraisal", [s.d.]). Em 2017, criou a *Cyber Diplomacy Toolbox*, uma ferramenta diplomática que faz parte da Política Externa e de Segurança Comum da UE, que colabora na prevenção de conflitos e na mitigação de ameaças, influenciando diretamente o comportamento de potenciais agressores ("The EU Cyber Diplomacy Toolbox", [s.d.]). O mecanismo permite que seus Estados-Membros, se necessário, tomem ações punitivas para responder, desencorajar ou dissuadir atividades maliciosas que visem prejudicar a integridade da UE. Como exemplo, em 2020, o Conselho, pela primeira vez, impôs uma série de sanções contra entidades e indivíduos responsáveis pelos ataques cibernéticos a uma de suas organizações ("*EU imposes the first ever sanctions against cyber-attacks*", [s.d.])

A Organização das Nações Unidas (ONU), embora atualmente envolvida no campo da segurança cibernética, não possui implementações diretamente ligadas ao desenvolvimento de respostas globais às ameaças digitais. Entretanto, a organização promove diálogos, comitês e marcos normativos para ajudar na regulamentação do ciberespaço, como o Grupo de Trabalho sobre Cibersegurança e Uso Pacífico do Ciberespaço (GGE). O grupo tem por objetivo reunir especialistas de diversos países na discussão de normas comportamentais dentro do ciberespaço, além de produzir relatórios sobre os princípios da segurança cibernética e o uso pacífico do ciberespaço (*SECRETARY-GENERAL; SECURITY, 2015*).

5. Considerações finais

Este trabalho teve por finalidade compreender o processo de securitização do ciberespaço como um novo domínio, com foco nos ataques cibernéticos à Estônia em 2007 e nos impactos provocados na política internacional. A análise buscou compreender como esse episódio gerou um debate global sobre segurança cibernética e crimes cibernéticos a partir da literatura revisada e do estudo de casos de medidas aplicadas por países e organizações internacionais.

Para se atingir um entendimento da relação entre criminalidade cibernética e segurança internacional, foram estipulados três objetivos específicos. O primeiro foi investigar a

influência do ataque cibernético à Estônia nas discussões globais sobre segurança cibernética e crimes cibernéticos. Verificou-se que o incidente estoniano evidenciou as vulnerabilidades na defesa de infraestruturas críticas e estimulou a inserção do ciberespaço nas agendas de segurança como uma área prioritária.

Em seguida, procurou-se analisar de que maneira países e organizações internacionais enquadraram a questão cibernética como uma ameaça, observando a securitização via cibersegurança, sendo identificado pelos atores políticos como uma ameaça existencial à segurança nacional e internacional. Por fim, o terceiro objetivo foi identificar as tomadas de respostas coletivas adotadas para enfrentar os crimes cibernéticos. Concluiu-se que iniciativas como a política de estratégia nacional estoniana, o Centro de Excelência de Defesa Cibernética Cooperativa da OTAN e a Diretiva NIS da União Europeia, foram respostas diretas no reconhecimento da cibersegurança como uma questão emergencial.

Com isso, confirma-se a hipótese de que o ataque à Estônia foi um catalisador para a criação de políticas e iniciativas de defesa cibernética internacional, visto que com os fatos apresentados, é evidente que o evento fomentou uma nova perspectiva sobre o ciberespaço, tratado desde então como um setor estratégico de segurança em ascensão. Assim, conclui-se que o ataque à Estônia em 2007 impulsionou não apenas novos debates sobre cibersegurança, mas também a implementação de respostas institucionais e medidas colaborativas que visam mitigar crimes cibernéticos no contexto global.

Os instrumentos de coleta de dados permitiram uma análise qualitativa da evolução das respostas institucionais, oferecendo uma visão detalhada das políticas e mecanismos de defesa cibernética implementados após o ataque estoniano. Portanto, sugere-se, em pesquisas futuras, utilizar-se do arcabouço da segurança cibernética para explorar o impacto de outras ameaças cibernéticas na securitização do ciberespaço e lidar com guerras híbridas a partir da eficácia das medidas adotadas em resposta aos ataques.

Referências

BRIEFING Implementation Appraisal. [s.l.: s.n.]. Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf.

BUZAN, Barry; HANSEN, Lene. A evolução dos estudos de segurança internacional. São Paulo: Editora Unesp, 2012.

BUZAN, Barry; WÆVER, Ole; WILDE, Jaap de. Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner Publishers, 1998.

CCDCOE. Disponível em: https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/#footnote_1_2663. Acesso em: 1 nov. 2024.

CCDCOE. Tallinn Manual 2.0. Disponível em: https://ccdcoe.org/research/tallinn-manual/.

CYBERDEFENSE REPORT. Estonia's National Cybersecurity and Cyberdefense Posture Policy and Organizations. [s.d.].

EU imposes the first ever sanctions against cyber-attacks. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

GAMERO-GARRIDO, A. Cyber conflicts in international relations: Framework and case studies. Mit.edu, 2014.

GEERS, K. Keynote Speech Cyberspace Changing Nature of Warfare. [s.l.: s.n.]. Disponível em: https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf.

HAATAJA, Samuli. The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. Law, Innovation and Technology, v. 9, n. 2, p. 159-189, 2017.

HANSEN, Lene; NISSENBAUM, Helen. Digital disaster, cyber security, and the Copenhagen school. International Relations, v. 26, n. 1, p. 118-135, 2012.

ILVES, Toomas Hendrik. Address by the President of Estonia. 62nd Session of the United Nations General Assembly, New York, 25 September 2007. Disponível em: http://www.un.org/webcast/ga/62/2007/pdfs/estonia-eng.pdf. Acesso em: 22 set. 2024.

KASKA, K.; OSULA, A.-M.; STINISSEN, J. The Cyber Defence Unit of the Estonian Defence League Legal, Policy and Organisational Analysis. [s.l.: s.n.]. Disponível em: https://nsarchive.gwu.edu/sites/default/files/documents/4060573/NATO-Cooperative-Cyber-Defence-Centre-of.pdf. Acesso em: 31 out. 2024.

NATO. Collective Defence and Article 5. Disponível em: https://www.nato.int/cps/en/natohq/topics_110496.htm.

NATO Cooperative Cyber Defence Centre of Excellence. Disponível em: https://mil.ee/en/landforces/ccdcoe/.

NATO. Cyber defence. Disponível em: https://www.nato.int/cps/en/natohq/topics_78170.htm.

NATO Speech: "Today's NATO, and why it matters" - Speech by NATO Secretary General, Jaap de Hoop Scheffer, Lloyd's City Dinner, London, 5 September 2007. Disponível em: https://www.nato.int/docu/speech/2007/s070905b.html. Acesso em: 28 out. 2024.

PERNIK, Piret; TUOHY, Emmet. Interagency Cooperation on Cyber Security: The Estonian Model. Tallinn: International Centre for Defence and Security, 2013.

Prime Minister Andrus Ansip's speech in Riigikogu. Disponível em: https://www.valitsus.ee/en/news/prime-minister-andrus-ansips-speech-riigikogu. Acesso em: 28 out. 2024.

ROLF, J. N. The first 100 years: IR, critical security studies and the quest for peace. International Politics, 19 maio 2022.

SECRETARY-GENERAL, U.; SECURITY, U. G. OF G. E. ON D. IN THE F. OF I. AND T. IN THE C. OF I.. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security :: note /: by the Secretary-General. digitallibrary.un.org, 22 jul. 2015.

SHAKARIAN, Paulo; SHAKARIAN, Jana; GUINN, Andrew. Introduction to Cyber-Warfare: A Multidisciplinary Approach. Amsterdam: Elsevier, 2013.

TANNO, Grace. A contribuição da Escola de Copenhague aos estudos de segurança internacional. Contexto Internacional, Rio de Janeiro, v. 25, n. 1, p. 47–80, jan./jun. 2003.

THE ECONOMIST. War in the fifth domain. Disponível em: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain. Acesso em: 23 out. 2024.

The EU Cyber Diplomacy Toolbox. Disponível em: https://www.cyber-diplomacy-toolbox.com/.

UNITED STATES. Department of Defense. Dictionary of Military and Associated Terms. Joint Publication 1-02, 8 nov. 2010 (As amended through 15 feb. 2016).

WÆVER, Ole. Securitization and Desecuritization. In: LIPSCHUTZ, Ronnie (Ed.). On Security. New York: Columbia University Press, 1995. p. 46-86.

WILLIAMS, Michael C. Words, images, enemies: Securitization and international politics. International Studies Quarterly, v. 47, n. 4, p. 511-531, 2003.