6

O CIBERTERRORISMO NO SÉCULO XXI: OS DESAFIOS DA CIBERSEGURANÇA

Stephanie Casanova Villela*

Resumo: Atualmente os ataques terroristas são cada vez mais sofisticados e com menos uso de violência física. Muitas organizações terroristas aperfeiçoaram os seus métodos e praticam os ataques de forma on-line. Esta nova forma de agressão é chamada de ciberterrorismo, essa prática se caracteriza como ataques cibernéticos que causam danos a um Estado e em sua população. Podem ser motivados pela política ou religião. O artigo pretende abordar essa prática de terrorismo cibernético, e os desafios que a cibersegurança enfrenta no século XXI. A metodologia do estudo é qualitativa, feita através de revisão de bibliografia, tendo como objetivo responder como ocorre o ciberterrorismo e quais os desafios da cibersegurança atualmente.

Palavras-chave: Ciberterrorismo. Cibersegurança. Ataques Cibernéticos. Terrorismo Cibernético. Organizações Terroristas.

Sumário:1. Introdução. 2. O ciberterrorismo no século XXI. 3. Os desafios da cibersegurança. 4. Estudo de casos. 4.1. Caso do Kosovo (1998). 4.2. Caso 11 de Setembro (2001). 4.3. Caso Wannacry (2017). 4.4. Casos que envolveram a Rússia. 5. Considerações finais. Referências.

CYBERTERRORISM IN THE 21ST CENTURY: CYBERSECURITY CHALLENGES

Abstract: Currently, terrorist attacks are increasingly sophisticated and with less use of physical violence. Many terrorist organizations have perfected their methods and carry out attacks on-line. This new form of agressão is called cyberterrorism, this practice is characterized as cyber attacks that cause damage to a state and its population. They can be motivated by politics or religion. The article intends to address this practice of cyber terrorism, and the challenges facing cybersecurity in the 21st century. The study methodology is qualitative, carried out through a review of the bibliography, aiming to answer how cyberterrorism occurs and what are the current cybersecurity challenges.

Keywords: Cyberterrorism. Cybersecurity. Cyber Attacks. Cyber Terrorism. Terrorist Organizations.

* Especialista em Direito Digital pela Fundação Escola Superior do Ministério Público (FMP) e Mestranda em Relações Internacionais pelo ISCSP – Universidade de Lisboa. *E-mails:* sc.villela@hotmail.com / scvillela95@gmail.com

Summary: 1. Introduction. 2. The Cyberterrorism in 21st Century. 3. The Challenges of Cybersecurity. 4. Study Cases. 4.1. Kosovo Case (1998). 4.2. 11 September Case (2001). 4.3. WannaCry Case (2017). 4.4. Cases Involving Russia. 5. Final considerations. References.

1 Introdução

Na atualidade, o conceito de terrorismo vem sendo cada vez mais ampliado. Atos de terrorismo não são somente físicos, também podem ser executados de forma *on-line*. Os grupos terroristas começaram a usar os computadores e a tecnologia para seus ataques, assim a sofisticação cresce cada vez mais. Nesse contexto, *hackers* com motivações políticas ou religiosas são recrutados por extremistas.

O ciberterrorismo é caracterizado como uma forma de impor terror por meio de ataques contra computadores e suas redes, informações armazenadas, serviços essenciais, sistema bancário entre outros, que causam pânico, acidentes e perdas econômicas.

É correto afirmar que a tecnologia trouxe diversos benefícios nos últimos anos e que antigamente o terrorismo se tratava somente de atos físicos. Desta forma, era muito mais fácil prevenir e combater tal ato, pois haviam fronteiras delimitadora dos Estados. Nos dias atuais, com a globalização da tecnologia, essas fronteiras não mais existem no mundo digital. Hoje um ataque perpetrado por hackers chineses pode parar um sistema eletrônico dos Estados Unidos. Um ataque contra bancos ou roubo de armazenamento de dados de forma *on-line* é possível sem necessidade de violência física, mas mesmo assim são muito prejudiciais aos Estados e suas populações.

A motivação principal para a escolha do tema do artigo está relacionada com o interesse da autora em Direito Penal Internacional, já que esta atualmente também faz Mestrado em Relações Internacionais no ISCSP – Universidade de Lisboa, e estágio na Corte Internacional Criminal em Haia, na Holanda. A autora também acredita que o tema do artigo é atualmente relevante devido ao crescente número e à modernidade de ataques cibernéticos detectados nos últimos tempos nas redes digitais. Isso dificulta a cibersegurança dos Estados e a proteção de seus dados.

Trata-se de uma pesquisa qualitativa e descritiva cuja metodologia será feita a partir de uma revisão bibliográfica. A principal pergunta de partida é: Como ocorre o ciberterrorismo e quais são os desafios da cibersegurança nos dias atuais? O artigo, além de elucidar essa questão, também contribuirá para o entendimento dessa forma mais recente de crime digital com o objetivo de explorar a questão em relação aos riscos que um sistema de cibersegurança deficiente pode causar ao Estado. Outrossim, serão abordados:

a) conceitos de ciberterrorismo e cibersegurança;
b) medidas para a prevenção de ciberataques;
c) como os Estados se protegem juridicamente do ciberterrorismo;
d) Estudos de casos.

2 O ciberterrorismo no século XXI

Hoje em dia, com a evolução da tecnologia, quando se trata de um ataque terrorista, já não se fala mais exclusivamente em atos violentos contra cidadãos civis. Por vezes, esse ataque é executado por um grupo terrorista a uma nação de forma *on-line* (GARDINI, 2014), sendo assim, "o ciberterrorismo resulta em termos simples da convergência do terrorismo e do ciberespaço e refere-se àquilo que se designa igualmente por 'terrorismo eletrônico'" (NOVAIS, 2012, p. 91). Essa nova forma de terrorismo, também chamada de terrorismo cibernético, caracteriza-se por uma forma de ciberataque a um governo ou instituição. Isso acontece porque o espaço cibernético simplifica o trabalho das organizações teorristas, uma vez que é possível manter o anonimato, o acesso é facilitado e o custo é baixo. Gardini define o ciberterrorismo como "ações de objetivos políticos ou religiosos que são realizadas por meio do espaço cibernético para causar graves danos contra a sociedade civil ou governos" (GARDINI, 2014, p. 18).

Para se ter sucesso em uma guerra, é necessário afetar a capacidade do inimigo. Uma estratégia usada é o planejamento de ataques conta infraestruturas críticas como centrais elétricas e sistemas de transporte que auxiliam nas ações de guerra do adversário. Nos dias atuais, um ciberataque pode ser considerado em nível estratégico se causar impacto suficiente para afetar a capacidade de funcionamento de um Estado, e esta estratégia ainda é mais barata e acessível do que qualquer ataque físico. Assim, ataques digitais podem causar grandes danos a um Estado por um valor bem mais baixo, e combinados com ataques físicos causam um prejuízo colossal. Um exemplo desta combinação foi no caso da guerra entre a Rússia e a Ucrânia.

Os grupos terroristas passaram a usar a tecnologia para os seus crimes como uma forma facilitadora de alcançar o seu objetivo. *Hackers* com motivações políticas ou religiosas são recrutados por extremistas para que difundam terror pelos meios digitais. Esses ataques podem ser entendidos contra:
a) computadores e suas redes;
b) informações armazenadas;
c) serviços essenciais ou infraestrutura como: sistema bancário, fornecimento de água ou energia elétrica, entre outros (RAPOSO, 2007).

O ciberterrorismo se tornou uma opção mais moderna de ataque terrorista, pois pode ser feito de forma anônima e causa danos imensos (WEIMANN, 2004).

Os principais métodos de terrorismo digital foram identificados como intimidação e coerção de autoridades públicas ou da população. Os objetivos do terrorismo digital são parecidos com os do terrorismo tradicional, tendo ambos - implicações políticas ou sociais. Um dos principais problemas para a ciência criminológica é a dificuldade de determinar o complexo causal do ato criminoso formado pelas suas causas e condições em relação, neste trabalho, ao terrorismo cibernético. "A primeira razão para o desenvolvimento do cibercrime em geral e do ciberterrorismo – em particular, é a possibilidade virtualmente ilimitada de financiá-los de pessoas que têm um interesse político, mercenário, ou outro em atingir os objetivos desses crimes" (SEREBRENNIKOVA, 2020).

Segundo o Relatório da UNODC[1] entitulado *The use of the internet for terrorist purposes*, existe uma classificação de seis etapas para o terrorismo cibernético:

- *Propaganda:* é uma forma de promover a ideologia terrorista entre usuários da internet;
- *Financiamento:* a internet também pode ser usada para financiar atos terroristas, como meio de coleta financeira, podendo ser feita por solicitação direta, comércio eletrônico, exploração de ferramentas de pagamento *on--line* e por meio de organizações de caridade;
- *Treinamento:* os terroristas têm cada vez mais recorrido à internet como um campo de treinamento para a execução de seus ataques. São disponibilizadas, em plataformas da internet, guias de como entrar nessas organizações terroristas e de como planejar e executar o ataque;
- *Planejamento:* diversos profissionais da justiça criminal citaram o uso da internet como sendo muito comum nos ataques terroristas. Dessa forma, o planejamento de um ato terrorista se baseia na comunicação de diversos sujeitos à distância, assim como na escolha do alvo do ataque;
- *Execução:* a internet pode ser usada na execução dos atos terroristas, podendo ser utilizadas ameaças de violência como forma de coordenar os ataques. Um exemplo onde a internet foi fortemente usada na coordenação dos participantes do ataque foi no 11 de setembro;
- *Ataques cibernéticos:* caracterizam-se pela utilização da internet para fazer um ataque. Geralmente essas investidas são para prejudicar o funcionamento de computadores, por meio de um vírus de computador, *malwares* e entre outros (UNODC, 2012).

[1] *United Nations Office on Drugs and Crime.*

Os ataques terroristas muitas vezes têm intenções políticas ou sociais, como ocorreu no ataque a Israel, em 2012, que envolveu diversos *sites* emblemáticos, como o da Bolsa de Valores de Tel Aviv e o da companhia aérea nacional, além da exposição sem autorização de dados de cartões de crédito e contas bancárias de diversos cidadãos israelenses (UNODC, 2012). Mas afinal, quem são esses ciberterroristas? Um ataque digital pode ser elaborado e executado por qualquer pessoa que entenda de tecnologia da computação e tenha motivos religiosos ou políticos para causar danos a outros grupos de pessoas. Podem ser tanto *hackers* amadores como profissionais e os ataques podem ser realizados por somente um indivíduo ou um grupo terrorista organizado. Segundo dados recolhidos pelo autor Shamsuddin Abdul Jalil em seu artigo *Countering Cyber Terrorism Effectively: Are We Ready To Rumble?*, 90% dos ciber criminosos são caracterizados por serem amadores, 9,9% são hackers profissionais com potencial para serem contratados, também conhecidos como espiões corporativos, e, por último, 0,1% são cibercriminosos de classe mundial (JALIL, 2003). Existem quatro tipos de terroristas:

1 – Terroristas com somente um foco: o motivos do ataque é decorrente de um assunto particular;
2 – Terroristas ideológicos: usam de violência para propagar a sua ideologia política;
3 – Terroristas nacionalistas: geralmente buscam se tornar independentes de um Estado ou entrar em um outro Estado por motivos éticos ou geográficos;
4 – Terroristas políticos religiosos: compreendem que seus atos são decorrentes de ordens divinas (ALCÂNTARA, 2015).

Existem diversos motivos para a realização de crimes digitais como o ciberterrorismo. Das razões para o ataque, destacam-se quatro principais:

1 – Destruir os sistemas operacionais de um inimigo: se caracteriza por uma forma fácil e barata para atacar o alvo e deixá-lo impossibilitado de operar;
2 – Arruinar com a reputação de uma nação, aliança ou organização: se trata de atacar a reputação da nação, aliança ou organização. Causa um impacto negativo na forma destas instituições operarem;
3 – Convencer as vítimas a trocar afiliação: força as vítimas a mudarem a sua afiliação ou associação a determinadas partes; e, por último,
4 – Para mostrar aos seus seguidores que eles têm o poder e são capazes de provocar danos significantes nos seus alvos: por vezes os cibercriminosos pretendem, com o ataque, provar aos seus seguidores e ao mundo que eles possuem meios e capacidades de cometer graves danos aos seus inimigos. Querem mostrar o seu poder ao mundo (JALIL, 2003).

Desde que se iniciaram os ataques terroristas por meios eletrônicos, os Estados começaram a se preparar para combater essa ameaça global. Desta forma,

foram elaborados meios para assegurar a proteção dos cidadãos e empresas. Assim, a legislação de cada Estado foi se adaptando para essa nova forma de ameaça. Segundo a ONU,[2] o ataque cibernético de um Estado contra o outro, ou de uma organização terrorista contra um Estado, pode ser considerado como uso de força, visto que pode desencadear um conflito armado internacional. Desta forma, o Estado atacado poderia se defender legitimamente por meio de um investida militar (GAMÓN, 2017). Outras estratégias também foram desenvolvidas para os Estados se protegerem dos atentados ciberterroristas:

1 – Processar os agressores: a parte atingida pelo ataque cibernético deve trabalhar para processar o seu agressor. Mostrar que este tipo de crime causa consequências jurídicas criminais pode desencorajar a prática deste crime;
2 – Desenvolver melhores práticas de segurança: as organizações internacionais e os Estados devem se certificar que possuem bons sistemas de segurança digital, assim, um ciberataque dependeria de bastante esforço para ser executado, muitas vezes não obtendo sucesso;
3 – Ser proativo: as pessoas em geral devem se comprometer a melhorar suas condutas em relação à segurança da informação. Devemos sempre nos informar de como esses ataques correm e o que podemos fazer para evitar;
4 – Desenvolver sistemas de seguranças vitas: incentivar o uso de sistemas como Sistemas de Detecção de Intrusão (IDS) e softwares de antivírus;
5 – Estabelecer planos de continuidade e recuperação: as organizações precisam ter planos de continuidade das atividades e de recuperação de dados em casos de desastres. Devem conter duas atividades essenciais: reparação e restauração. A reparação deve resolver o problema e a restauração deve ser ativada com cooperações antecipadamente especificadas com fornecedores de software, hardware, etc;
6 – Cooperação com diversas firmas e grupos de trabalhos: as organizações devem estabelecer vínculos trabalhistas e acordos com entidades públicas e privadas que podem ajudar com danos causados pelo ciberterrorismo;
7 – Aumentar a conscientização em relação à segurança: educar a população para se proteger de ataques cibernéticos e a ser mais proativa em questões de cuidar da segurança da informação;
8 – Leis cibernéticas mais rígidas: devem ser desenvolvidas leis e punições mais severas para casos de ciberataques;
9 – Incentivar a pesquisa e o desenvolvimento: devem ser apoiadas as pesquisas e desenvolvimentos de projetos que encorajem o desenvolvimento de estudos que busquem melhorar a qualidade dos sistemas de defesa da informação (JALIL, 2003).

[2] Organização das Nações Unidas.

Klimburg, citado por Fernandes (2012), faz uma analogia entre o cibercrime, ciberterrorismo e ciberguerra. Ele acredita que os três elementos citados dividem as mesmas redes sociais e podem ter objetivos similares. Segundo Klimburg, o cibercrime apresenta uma base técnica, como, por exemplo, o *software* e o apoio logístico, já o ciberterrorismo proporciona a base social, como as redes pessoais e a motivação, elementos que podem levar a ataques às redes de computadores de inimigos ou nações. Desta forma, alguns governos optam por preservar o que se chama por "organizações por procuração". Essas seriam capazes de ser comprometidas em ações de ciberataque e, por vezes, em atividades de ciberdefesa (FERNANDES, 2012).

Uma pergunta interessante para os ciberataques é em relação às responsabilidades, levando em conta os meios técnicos necessários: quais ciberataques pudessem decorrer de iniciativas de agentes não governamentais e à margem dos Estados? Esse tipo de ciberataque percebe-se que somente pode ocorrer com o apoio ou a aprovação de um governo, mesmo que neguem qualquer envolvimento. Segundo Klimburg, novamente citado por Fernandes (2012), ataques menos sofisticados como ataques de negação de serviço ou em que apagam páginas na internet são realizados por grupos não governamentais, porém, atuam com o seu suporte técnico (*Ibidem*).

Outra questão interessante em relação ao ciberterrorismo é a relação com a mídia. Cádima afirma que o sucesso dos atentados terroristas têm relação com a publicidade concedida pela mídia, "apesar de uma progressiva desterritorialização da utilização por parte dos grupos terroristas para as plataformas digitais, reapossando-se das funções habituais dos média convencionais e complementadas com novas competências" (CÁDIMA, 2017, p. 73). A mídia consiste em um alvo ou um recurso para as organizações terroristas.

Essa relação entre a mídia e o terrorismo consiste no incentivo que a mídia dá ao terrorismo, na forma que os terroristas buscam por atenção. Quanto mais a mídia noticia os ataques, mais os grupos terroristas se sentem motivados a cometê-los. Por outro lado, a mídia também é considerada uma vítima de terrorismo.

Em relação ao terrorismo cibernético e a mídia em específico, "o uso da internet veio reforçar a possibilidade da promoção da propaganda, e nalguns casos contrariar e circum-navegar os *media* convencionais" (NOVAIS, 2012, p. 98). A internet permite uma fácil e rápida comunicação, promovendo a globalização, fazendo com que os terroristas estejam presentes em qualquer lugar proporcionando mais oportunidades de recrutamento.

3 Os desafios da cibersegurança

É inegável que a tecnologia mudou o mundo e a sociedade, permitindo o desenvolvimento de uma sociedade virtual no ciberespaço. Para o Estado soberano, o processo de decisão tem sofrido dificuldades de se adaptar ao sistema internacional, diferenciando-se de como os interesses nacionais do Estado eram defendidos antigamente. Isso decorre da globalização e da dificuldade em lidar com os fluxos de informação. Dessa forma, a dificuldade de filtrar esse fluxo de informações que passa pelo espaço cibernético torna o sistema mais vulnerável (MARTINS, 2012). Assim, o principal problema da cibersegurança é do valor da informação, "na sua aceção de preocupação pela salvaguarda da informação nacional vital, essencial e confidencial, tendo em vista o interesse nacional" (LEITE, 2016, p. 5).

O ciberespaço está aberto a todos e, nas últimas duas décadas, o número de usuários da internet aumentou exorbitantemente. Infelizmente e indiscutivelmente, a internet pode ser usada como uma arma para conflitos estatais e não estatais. O espaço virtual é acessível a todos e pode causar tantos danos quanto o terrorismo tradicional. Da mesma forma que a internet é essencial na atualidade, ela também tornou a população mais vulnerável (VIANA, 2012). A tecnologia abriu o mundo para novas realidades sem fronteiras, o que, consequentemente, impactou na segurança visto que qualquer pessoa ou programa de computador podem interagir entre si com motivações ilegais, sendo muito importante a atuação da Defesa Nacional para a proteção do Estado. Os Estados passaram a precisar desenvolver políticas públicas de segurança com o objetivo de garantir a sua Segurança Nacional no ciberespaço (LEITE, 2016).

Alguns dos principais desafios enfrentados pela cibersegurança são:

1 – a programação ineficiente que deixa aberta a chance de haver vulnerabilidades no *software*;
2 – a falta de informação, na maioria das vezes os usuários do *software* entendem menos de como usá-lo do que quem o desenvolveu, assim o deixa vulnerável;
3 – o fácil acesso à internet, ou seja, se muitas pessoas tem acesso à internet, mais crimes podem ser cometidos;
4 – leis ineficientes: é necessário que cada Estado desenvolva leis domésticas mais eficientes e participem de tratados internacionais acerca do assunto (SEN, 2018).

As grandes potências mundiais e alguns estados menores estão desenvolvendo uma nova política chamada de "Políticas de Informação" com estratégias integradas que buscam expandir a sua rede de informações, para que possa ser

disponibilizado um melhor sistema de segurança da informação e possibilitar o livre acesso ao espaço cibernético.

Deve-se recordar que a internet é a base dos sistemas de informação entre os Estados, Forças Armadas e Serviços de Informação e de Segurança, sistemas que são alvos de ataques por terroristas extremistas e que, quando atacados, colocam em risco o funcionamento de um Estado e os seus interesses nacionais. Dessa forma, torna-se imprescindível a elaboração de estratégias de segurança e defesa com o objetivo de garantir a liberdade de ação no ciberespaço de forma segura (VIANA, 2012). Nunes (2012) partilha da mesma declaração, em que acredita que o Estado deve "desenvolver uma 'Política para o Domínio da Informação' que permita garantir, não só a convergência estrutural para os parâmetros tecnológicos da Sociedade da Informação e do Conhecimento, como também a Segurança e a Defesa da sua Infraestrutura de Informação" (NUNES, 2012, p. 118).

Atualmente, a internet não possui uma nacionalidade ou uma lei internacional que proíba a livre circulação. Entretanto, existem alguns casos peculiares como o da Coreia do Norte, onde o acesso à internet é proibido à população, ou da China, que bloqueia determinadas páginas sempre que sente alguma ameaça que possa atacar o seu interesse nacional, sendo considerada uma violação da liberdade. As atitudes desses dois governos consistem em limitar a circulação de informações para que as suas estruturas governamentais não possam ser atacadas ou para que o resto do mundo não tenha conhecimento do que ocorre em seus territórios. Entretanto, vale destacar que a internet não reflete uma infraestrutra aberta e descentralizada, pois as conexões são feitas via satélite, companhias de telecomunicações, etc.

Apesar de se tratar de uma realidade virtual, a internet depende de estruturas físicas. Dessa forma, existe uma possibilidade de regular o tráfego de informações pela utilização de filtros e de programas informáticos de vigilância devido a razões políticas ou econômicas. Um exemplo de limitação é a da Índia, que impede o acesso a conteúdos islâmicos e hindus extremistas (MARTINS, 2012). Assim, os Estados possuem uma função relevante no espaço cibernético, pois mesmo o ciberespaço sem fronteiras submete-se a estruturas físicas situadas em territórios que possuem a sua própria legislação. Assim, o espaço geográfico passa a ser importante e os governos podem desenvolver diversos projetos de segurança, como a educação para a cibersegurança e a criação de uma legislação específica (MONIZ, 2019).

O ciberespaço não pertence e não é administrado por governos, mas por diversos utilizadores de uma sociedade de informação globalizada. Em função do rápido crescimento das Tecnologias da Informação e Comunicação (TICs), o

espaço cibernético permanece em constante mutação. Dessa forma, os elementos tradicionais de regulamentação e soberania praticados pelos Estados com o objetivo de diminuir os perigos decorrentes do ciberespaço são complexos de serem implementados. Entretanto, para Nunes: "garantir a segurança do ciberespaço (cibersegurança) constitui hoje um imperativo nacional, essencial para garantir a soberania e a sobrevivência do país" (NUNES, 2012, p. 116). É importante analisar as vulnerabilidades estratégicas e as possíveis ameaças presentes no espaço cibernético, sendo necessária a elaboração de uma Estratégia Nacional de Cibersegurança (*Ibidem*).

A cibersegurança, tem como objetivo combater o cibercrimes e o hacktivismo.[3] Existe também a cibersegurança ligada aos serviços informáticos, como é o caso da ciberespionagem e do ciberterrorismo. "O ciberterrorismo, para que seja considerado como tal, tem de observar dois critérios cumulativos: o de apresentar uma motivação política e o de desencadear um resultado destrutível fisicamente visível" (LEITE, 2016, p. 6). Para se precaver dos crimes cibernéticos, como o ciberterrorimo, temos dois tipos de prevenção: a cibersegurança, que conta com a ação das forças policiais e dos serviços informáticos, e a ciberdefesa, que procede exclusivamente das forças armadas. Assim, a cibersegurança "tem como função a garantia da realização de missões de segurança e defesa nacional, ou seja, garantir uma soberania do estado no ciberespaço global" (*Ibidem*, p. 7), possibilitando ações antecipadas para evitar ciberataques. Já a ciberdefesa está interligada com o ciberterrorismo. Pode ser determinado como a utilização do ciberespaço para a conduta de atos terroristas (Ibidem).

"A Segurança Nacional começa em casa" (CALDAS; FREIRE, 2013). Não basta somente nos sentirmos seguros dentro das nossas fronteiras físicas, devemos também estar seguros no ciberespaço. Para manter o ciberespaço seguro é necessário ter o conhecimento de quais informações devem ser protegidas e desenvolver uma estratégia de defesa da informação. Deve haver um plano de proteção de infraestruturas críticas, no qual devem ser abordadas as seguintes questões: a caracterização de uma infraestrutura crítica; se possui conexão com a internet; se depende de tecnologias de informação; saber se caso seja perdida, se pode ameaçar a Segurança Nacional; se houver uma falha, existe a possibilidade de ser recuperado (*Ibidem*).

O Brasil já enfrentou situações desafiadoras de prevenção ao ciberterrorismo. Um desses grandes desafios foi em questão à prevenção de ciberataques durante as Olimpíadas de 2016. O Brasil estava em evidência internacional, momento esperado por terroristas. Desta forma, preservar a segurança das In-

[3] Ato de escrever um código fonte para promover uma ideologia.

fraestruturas Críticas e dos vínculos cibernéticos era essencial. Para isso, foram identificadas quatro medidas que o Brasil deveria tomar para a eficácia da proteção contra terrorismos durante o evento:

1 – a necessidade de uma lei interna que tipificasse o conceito de terrorismo para o Brasil;
2 – o desenvolvimento de uma cultura de proteção nesta área, tanto físico quanto virtual;
3 – assegurar a expansão das comunicações digitais em nível nacional e internacional;
4 – fortalecer as instituições responsáveis pelas decisões em relação às ações antiterrorismo (ALCÂNTARA, 2015).

Sendo a arma usada pelos ciberterroristas o computador, o qual é facilmente acessível, a principal questão seria sobre como se proteger das organizações terroristas visto que não é possível a proibição de uso de computadores. Desse modo, é necessário haver leis que abordem o uso destas máquinas para atos ilícitos (GORDON; FORD, 2002). No Brasil, o ciberterrorismo é regulamentado pela Lei Antiterrorismo nº 13.260 de 2016. Seu artigo 2, inciso IV, diz que "sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou **servindo-se de mecanismos cibernéticos**, do controle total ou parcial, ainda que de modo temporário […]" (BRASIL, 2016, grifo nosso).

Compete à Polícia Federal a investigação e à Justiça Federal o julgamento e processamento dos crimes de terrorismo. Conforme está descrito no art. 11 da Lei nº 13.260/16:

> Para todos os efeitos legais, considera-se que os crimes previstos nesta Lei são praticados contra o interesse da União, cabendo à Polícia Federal a investigação criminal, em sede de inquérito policial, e à Justiça Federal o seu processamento e julgamento, nos termos do inciso IV do art. 109 da Constituição Federal (BRASIL, 2016).

A pena prevista para esse tipo de crime no Brasil consiste em reclusão de doze a trinta anos, além das sanções análogas aos crimes de ameaça ou violência. Assim, observa-se que o Brasil apresenta uma regulamentação válida para essa prática criminal, porém, não uma legislação específica, mas leis que alteram o Código Penal.

Já a União Europeia possui uma lei específica somente para o combate à cibercriminalidade, que é a Resolução do Parlamento Europeu, de 3 de outubro de 2017, sobre a luta contra a cibercriminalidade (2017/2068(INI)) (PARLAMENTO EUROPEU, 2017). Também foi aprovada a Diretiva Segurança das Redes e da Informação (SRI) em maio de 2018, que tem como objetivo identificar os operadores de serviços essenciais e instituir o dever de comunicar os incidentes de segurança digital às autoridades competentes (IMMENKAMP *et al.*,

2019). Com esta Diretiva, os países-membros da União Europeia estão preparados para lidar com ciberataques de forma que:

1 – indiquem às autoridades competentes;
2 – criem grupos de repostas a incidentes de segurança informática;
3 – desenvolvam estratégias nacionais de cibersegurança (PARLAMENTO EUROPEU, 2016).

Em 2019, também foi aprovado um ato legislativo distinto que reforçou a Agência da União Europeia para a Segurança da Informação das Redes (ENISA), que tem como objetivo desempenhar um papel mais amplo em relação à cibersegurança da União Europeia (PARLAMENTO EUROPEU, 2019).

Os Estados Unidos também adotaram medidas mais agressivas ao combate do terrorismo e ciberterrorismo. Desta maneira, qualquer indivíduo que cometa um crime que se encaixe nas descrições de terrorismo não são apresentados a um juiz, mas sim a uma Comissão Militar indicada pelo Presidente dos Estados Unidos ou pelo Secretário de Defesa. Este processo não é público e pode ser aplicada a pena de morte (NUNES; LEHFELD; SILVA, 2020).

4 **Estudo de casos**

4.1 Caso do Kosovo (1998)

A guerra do Kosovo teve início em 1998, primeiramente envolvendo a Iugoslávia e o Exército de Libertação do Kosovo e, depois, a Organização do Tratado do Atlântico Norte (OTAN). Essa foi a primeira guerra onde houve participação significativa no ciberespaço. Assim, foi considerada uma das primeiras guerras cibernéticas. A Iugoslávia se reuniu em pequenos grupos com a intenção de atacar os *sites* da OTAN, servidores ou qualquer outra infraestrutura da OTAN ou dos países membros. Um grupo famoso que realizou ataques cibernéticos durante os bombardeios foi o *Black Hand*, com ataques em sites albaneses no Kosovo (MILOŠEVIĆ, 2014).

Os governos e instituições não governamentais utilizaram a internet e o ciberespaço para divulgar mensagens de propaganda, difamar os inimigos políticos e de guerra e também para desenvolver posições mais fortes. Os sistemas governamentais e os computadores da OTAN sofreram ataques de negação de serviços e bombas de *e-mails*. Esse ataque foi assumido pelo grupo *Black Tigers* (GIANTAS; STERGIOU, 2018).

4.2 Caso 11 de Setembro (2001)

Um dos grupos terroristas mais conhecidos de todos os tempos, Al Qaeda, já demonstrou interesse no uso da tecnologia como forma de ataque e com o objetivo destruir a economia dos Estados capitalistas. A preocupação é em relação à nova geração de terroristas, que atualmente cresce em um mundo digital e aprende que o uso de ferramentas de hacking pode ser mais poderoso, simples de usar e de fácil acesso. O ciberterrorimo pode se tornar mais cativante à medida que os mundos real e virtual se tornam mais próximos. Um exemplo é quando um grupo terrorista explode uma bomba no território alvo e os *hackers* atacam as estruturas de comunicação, impedindo assim a transmissão do evento.

Um exemplo muito famoso de ataque terrorista foi o 11 de setembro, quando a Al Qaeda usou recursos cibernéticos para recolher informações sobre os voos e formas de se comunicarem entre si durante os ataques. Existem algumas formas de disfarçar os planos de atentados terroristas na internet e um desses métodos é a esteganografia, que se caracteriza por ocultar mensagens em arquivos gráficos (THE UNITED STATES INSTITUTE OF PEACE, 2021). Segundo Gamón em sua obra *Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad:*

> Los crímenes del ciberterrorismo, cuando tienen intención de causar pánico colectivo, una alarma social generalizada, responden a una motivación ideológica determinada, conllevan implicaciones más graves que los delitos comunes para la seguridad nacional y la política de defensa (GAMÓN, 2017, p. 85).

4.3 Caso Wannacry (2017)

Em 2017, um ataque virtual atingiu 200 mil pessoas em 150 países diferentes. Os ataques incluíram alvos como hospitais públicos e bancos. Uma das piores consequências deste ataque foi em relação à saúde. As ambulâncias mudaram de rota e não foram capazes de atender pessoas que precisavam de cuidados urgentes e 19 mil consultas foram canceladas. O malware foi lançado contra os computadores, em geral com o propósito de extorquir dinheiro, e se caracterizou por um sistema que criptografa os dados contidos no computador que somente é descodificado mediante pagamento em bitcoins. Nesses casos, o pagamento é sempre desencorajado porque mesmo sendo pago não se pode ter certeza que os criminosos irão devolver os dados e isso pode incentivar mais ciberataques no futuro.

Alguns dor principais motivos pelos quais as pessoas não conseguiram se proteger destes ataques incluem:

1 – o sistema *Microsoft Windows* não estava atualizado;

2 – falta de treinamento dos funcionários que deveriam ser alertados para não clicar em links suspeitos e abrir anexos de email não confiáveis;
3 – não tinham um *software* de segurança devidamente instalado;
4 – não foram feitos *backups* dos dados.

Os Estados Unidos se manifestaram sobre o assunto acusando a Coréia do Norte de cometer os ataques cibernéticos. O ataque teria sido cometido por um grupo chamado Lazarus e seria o mesmo responsável, segundo os Estados Unidos, por atacar a Sony Pictures Entertainment em 2014, destruindo documentos e vazando informações corporativas na internet. Essas acusações surgiram durante o momento em que havia uma grande preocupação acerca da capacidade dos *hackers* na Coreia do Norte e o seu programa de armas nucleares (VOLZ, 2017). No início, o ataque parecia uma campanha de *ransomware*, quando *hackers* criptografam um computador alvo e exigem pagamento para recuperar arquivos. Alguns especialistas entenderam que a ameaça de resgate pode ter se tratado de uma distração com o objetivo de disfarçar uma intenção mais destrutiva (*Ibidem*).

4.4 Casos que envolveram a Rússia

Em abril de 2015 houve um ataque executado por *hackers* russos contra a TV5 francesa. Consistiu em um caso de *Advanced Persistent Threat*, que conseguiu deixar indisponíveis onze canais de TV5 na França, também, difundiu mensagens de reivindicações islâmicas na mídia pela internet, além de bloquear os meios tecnológicos do canal (MONIZ, 2019).

Um caso mais recente, que ocorreu no início de 2022, trata-se da Ucrânia e a Rússia. A Rússia atualmente está atacando a Ucrânia tanto de forma física, com bombardeios, quanto de forma digital. Antes do governo russo iniciar uma guerra física com a Ucrânia, ele começou a usar de ataques cibernéticos, provocando uma guerra digital. Além da população ucraniana ter que se preocupar com os bombardeios em seu território, passaram a ter que se preocupar também com o terror de uma guerra híbrida (SUZUKI, 2022). O uso da tecnologia foi utilizado para gerar pânico na população quando diversas páginas do governo ucraniano ficaram inacessíveis. Kiev acusou Moscou de um ciberataque, alegando ter provas. A União Europeia e a OTAN condenaram o ciberataque à Ucrânia, e o Secretário-Geral da OTAN se reuniu com o governo ucraniano para assinar um acordo de cooperação cibernética. Esse acordo tinha como objetivo ampliar e fortalecer a cooperação contra ataques cibernéticos (EXPRESSO, 2022). A ONU informou que as autoridades ucranianas também estão relatando um novo ataque cibernético em grande escala contra várias instituições estatais e financeiras (UN NEWS, 2022). Entretanto, em 24 de fevereiro

de 2022, a Rússia declarou guerra à Ucrânia. Nas últimas semanas, a Ucrânia tem sofrido diversos ataques russos. Além de ataques físicos, por meio de bombas e armas bélicas, também foram reportados ataques cibernéticos, tendo como alvos ministérios e bancos da Ucrânia. Essa é uma forma de guerra híbrida que pretende semear confusão (HARDIN *et al.*, 2022).

Todavia, essas duas vezes não foram as primeiras que a Rússia se envolveu em ciberataques. Em 2007 houve uma séries de ciberataques contra a Estônia devido à retirada de um monumento da guerra soviética em Tallin. Os ataques foram direcionados a *sites* do governo, empresas e bancos do país Báltico, porém, a Rússia negou qualquer envolvimento (SHEETER, 2007).

5 Considerações finais

Atualmente, ataques cibernéticos vêm aumentando consideravelmente devido a sua praticidade e baixo custo. A arma de quem pratica um ataque digital é o computador, e o objetivo é a intimidação e coerção de autoridades públicas ou da população, contendo implicações políticas, sociais ou religiosas.

Quando se trata de ciberterrorismo, o principal problema é o valor da informação e a dificuldade de proteger os dados. Os Estados precisam proteger o seus interesses nacionais, o que também abrange a área cibernética de proteção de dados.

O ciberterrorismo primeiro corre por propaganda pela qual são espalhadas as ideias terroristas com o objetivo de recrutar pessoas para executá-los. Esse recrutamento pode ser *on-line*, o que traz benefícios para a organização terrorista, pois pode se espalhar rapidamente pelo mundo todo. Outrossim, a internet é uma ferramenta essencial quando se trata de busca pelo financiamento, pois mesmo que os ataques sejam feitos de forma *on-line*, são necessários recursos. O planejamento dos ataques também usa de meio digital visto que ao planejar um ato terrorista é preciso haver comunicação a distância com diversos sujeitos, assim como na escolha do alvo do ataque. E, por fim, na execução: quando um ataque terrorista é feito digitalmente trata-se de ciberterrorismo.

Com o objetivo de combater este tipo de crime, os governos desenvolveram meios de segurança, mais conhecidos como cibersegurança, que combatem os cibercrimes e o hacktivismo. Logo, os governos desenvolveram políticas de informação visando melhorar a segurança dos sistemas de informação. Como se trata de um tipo de crime muito recente, devido ao uso da internet somente ter iniciado há alguns anos, esse sistema vem sendo desenvolvido e aperfeiçoado, o que desafia a capacidade dos Estados de se defenderem de ataques digitais.

Além destes meios de segurança, é importante lembrar que cuidados básicos no dia a dia também podem ajudar a prevenir ataques cibernéticos, como o uso de antivírus adequado, sempre atualizar o sistema, educar os usuários corretamente, trocar de senhas regularmente e não escolher senhas fáceis, fazer *backups*, não abrir *links* suspeitos e nunca conectar um pendrive desconhecido no computador usado para o trabalho. Estes pequenos cuidados muitas vezes podem evitar grandes catástrofes cibernéticas.

No meio jurídico, algumas leis abordam o assunto como forma de ajudar no combate ao terrorismo cibernético. A Europa e os Estados Unidos se encontram mais desenvolvidos no assunto. Ambos tomaram medidas mais agressivas em relação ao combate ao terrorismo digital, desenvolvendo leis específicas e comissões especiais para o julgamento de ciberataques. No Brasil, o ciberterrorismo é regulamentado pela Lei Antiterrorismo nº 13.260 de 2016, que em seu artigo 2, inciso IV, traz pena prevista de reclusão de doze a trinta anos, além das sanções análogas aos crimes de ameaça ou violência (BRASIL, 2016). Assim, podemos observar que o Brasil apresenta uma regulamentação válida para combate a essa prática criminal, no entanto, não uma legislação específica, mas sim lei que altera o Código Penal.

Referências

ALCÂNTARA, B. T. Brasil e ciberterrorismo: desafios para o Rio 2016. *The Ninth International Conference On Forensic Computer Science – ICoFCS 2015*, Brasília, p. 84-89, 2015. DOI: 10.5769/C2015011. Acesso: 13 out. 2022.

BRASIL. *Lei nº 13.260 de 16 de março de 2016.* Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis nº 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. *Leis Ordinárias*, Brasília, 2016. Disponível em: <https://bit.ly/3qhaoq5>>. Acesso em: 13 out. 2022.

CÁDIMA, F. R. Terrorismo e media. *Janus online*. Lisboa, 2017. Disponível em: <https://bit.ly/3iuKQBL>. Acesso em: 13 out. 2022.

CALDAS, A.; FREIRE, V. Cibersegurança: das preocupações à Ação. *National Defense Institute of Portugal*, Lisboa, 2013. *E-book.* Disponível em: <https://bit.ly/3CVBMPG>. Acesso em: 13 out. 2022.

EXPRESSO. Ucrânia: NATO e Kiev assinam acordo de cooperação cibernética após ataque informático. *Internacional*, Paço de Arcos, 17 jan. 2022. Disponível em: <https://bit.ly/3JnhUaw>. Acesso em: 13 out. 2022.

FERNANDES, J. P. T. A ciberguerra como nova dimensão dos conflitos do século XXI. *Relações Internacionais*, Lisboa, n. 33, p. 53-69, 2012. Disponível em: <https://bit.ly/3IiKdWj>. Acesso em: 13 out. 2022.

GAMÓN, V. P. Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad*, Quito, n. 20, p. 80-93, 2017. Disponível em: <https://doi.org/10.17141/urvio.20.2017.2563>. Acesso em: 13 out. 2022.

GARDINI, M. B. Terrorismo no ciberespaço: o poder cibernético como ferramenta de atuação de organizações terroristas. *Fronteira*, Belo Horizonte, v. 13, n. 25 e 26, p. 7-33, 2014. Disponível em: <https://bit.ly/3JlXRcC>. Acesso em: 13 out. 2022.

GIANTAS, D.; STERGIOU, D. From Terrorism to Cyber-terrorism: The Case of ISIS. *Social Science Research Network – SSRN*, Rochester, 2018. Disponível em: <https://bit.ly/3IaE4ve>. Acesso em: 13 out. 2022.

GORDON, S.; FORD R. (2002) Cyberterrorism? *Computers & Security*, v. 21, issue 7, p. 636-647, Amsterdam, 2002. DOI: https://doi.org/10.1016/S0167-4048(02)01116-1>. Acesso em: 13 out. 2022.

HARDIN, L. *et al.* Ukraine fighting to stop 'a new iron curtain' after Russian invasion. *The Guardian*, Kyiv, 24 fev. 2022. Disponível em: <https://bit.ly/3CSPvqh>. Acesso em: 13 out. 2022.

IMMENKAMP, B. *et al.* A luta contra o terrorismo. *Parlamento Europeu.* PE 635.561, Estrasburgo, 2009. Disponível em: https://what-europe-does-for-me.eu/data/pdf/ focus/focus01_pt.pdf>. Acesso em: 13 out. 2022.

JALIL, S. A. Countering Cyber Terrorism Effectively: Are We Ready To Rumble? *GIAC Security Essentials Certification (GSEC), Practical Assignment.* Versão 1.4b, Opção 1, Rockville Pike: 2003.

LEITE, A. M. X. F. A problemática da cibersegurança e os seus desafios. *CEDIS Working Papers*, n. 49, Lisboa, 2016. Disponível em: <https://bit.ly/3u5IpL1>. Acesso em: 13 out. 2022.

MARTINS, M. Ciberespaço: uma Nova Realidade para a Segurança Internacional. Instituto da Defesa Nacional. In: *Nação e Defesa*, n. 133, p. 32-49, Lisboa, 2012. Disponível em: <https://bit.ly/3Ilnvg3>. Acesso em: 13 out. 2022.

MILOŠEVIĆ, N. Case of the cyber war: Kosovo conflict. *Inspiratron*, Belgrade, 2014. Disponível em: <https://bit.ly/3qhfW3P>. Acesso em: 13 out. 2022.

MONIZ, P. Terrorismo e Violência Política: Como Combater o Ciberterrorismo e a Radicalização. *Instituto da Defesa Nacional*. In: Nação e Defesa, n. 152, p. 58-77, Lisboa, 2019. Disponível em: <https://bit.ly/3KUcFiR>. Acesso em: 13 out. 2022.

NOVAIS, R. A. Media e (Ciber)Terrorismo. Instituto da Defesa Nacional. In: *Nação e Defesa*, n. 133, p. 89-103, Lisboa, 2012. Disponível em: <https://bit.ly/3Ilnvg3>. Acesso em: 13 out. 2022.

NUNES, D. H.; LEHFELD, L. S.; SILVA, J. S. Ciberterrorismo e soberania: análise da Operação Hashtag como ato atentatório ao Estado. *Revista Videre*, v. 12, n. 24, maio/ago., Dourados, 2020. ISSN: 2177-7837. DOI: https://doi.org/10.30612/videre.v12i24.11075>. Acesso em: 13 out. 2022.

NUNES, P. F. V. A Definição de uma Estratégia Nacional de Cibersegurança. *Instituto da Defesa Nacional.* In: Nação e Defesa, Lisboa, n. 133, p. 113-127, 2012. Disponível em: <https://bit.ly/3Ilnvg3>. Acesso em: 13 out. 2022.

PARLAMENTO EUROPEU. Diretiva (Ue) 2016/1148 do Parlamento Europeu e do Conselho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. *Jornal Oficial da União Europeia*, Estrasburgo, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri= CELEX :32016L1148&from=PT>. Acesso em: 13 out. 2022.

PARLAMENTO EUROPEU. Luta contra a cibercriminalidade. Resolução do Parlamento Europeu, de 3 de outubro de 2017, sobre a luta contra a cibercriminalidade (2017/2068(INI)). *Jornal Oficial da União Europeia*, Estrasburgo, 2017. Disponível em: <https://www.europarl.europa.eu/doceo/document/TA-8-2017-0366_PT.pdf>. Acesso em: 13 out. 2022.

PARLAMENTO EUROPEU. ENISA and a new cybersecurity act. *EU legislação em progresso*, Estrasburgo, 2019. Disponível em: <https://www.europarl.europa.eu/RegData/ etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf>. Acesso em: 13 out. 2022.

RAPOSO, A. C. Terrorismo e contraterrorismo: desafio do século XXI. *Revista Brasileira de Inteligência*, v. 3, n. 4, p. 39-56, 1º set. 2007. Disponível em: <https://bit.ly/3tiaP5w>. Acesso em: 13 out. 2022.

SEN, R. Challenges to cybersecurity: current state of affairs. *Communications of the Association for Information Systems*, v. 43, article 2, Atlanta, 2018. ISSN:1529-3181. DOI: 10.17705/1CAIS.04302. Disponível em: <https://aisel.aisnet.org/cais/vol43/iss1/2>. Acesso em: 13 out. 2022.

SEREBRENNIKOVA, A. V. Cyber terrorism: modern challenges. *Colloquium*, n. 19, v. 71, Moscou, 2020. Disponível em: <https://cyberleninka.ru/article/n/cyber-terrorism-modern-challenges>. Acesso em: 13 out. 2022.

SHEETER, L. Estônia acusa Rússia de "ataque cibernético" ao país. *BBC Brasil*, São Paulo, 17 maio 2007. Disponível em: <https://bbc.in/36ut3I4>. Acesso em: 13 out. 2022.

SUZUKI, S. A guerra cibernética paralela entre Rússia e Ucrânia. *BBC News Brasil*, São Paulo, 1 março 2022. Disponível em: <https://www.bbc.com/portuguese/internacional-60551648>. Acesso em: 13 out. 2022.

THE UNITED STATES INSTITUTE OF PEACE. Terror on the Internet: Questions and Answers. *Analysis and Commentary*, Washington, DC, 2021. Disponível em: <https://bit.ly/3N2dlV4>. Acesso em: 13 out. 2022.

UN NEWS. AS Security Council meets on Ukraine crisis, Russia announces start of 'special military operation'. *United Nations Website*, Nova Iorque, 24 fev. 2022. Disponível em: <https://bit.ly/3N2QQ2A>. Acesso em: 13 out. 2022.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). *The use of the internet for terrorist purposes*. Vienna, 2012. Disponível em: <https://bit.ly/3ihGAoR>. Acesso em: 13 out. 2022.

VIANA, V. R. Editorial. Instituto da Defesa Nacional. In: *Nação e Defesa*, n. 133, p. 5-7, Lisboa, 2012. Disponível em: <https://bit.ly/3Ilnvg3>. Acesso em: 12 jan. 2022.

VOLZ, D. U. S. blames North Korea for 'WannaCry' cyber attack. *Reuters*, Londres, 18 dez. 2017. Disponível em: <https://reut.rs/3CUWxL9>. Acesso em: 13 out. 2022.

WEIMANN, G. www.terror.net: How Modern Terrorism Uses the Internet. *United States Institute of Peace*, Washington, DC, 2004. Disponível em: <https://bit.ly/3JFnzZy>. Acesso em: 13 out. 2022.