LILIAN DILL DONATI GODINHO

CIBERTERRORISMO: A NOVA GUERRA FRIA?

Orientador: Professor Doutor José Filipe Pinto

Universidade Lusófona – Centro Universitário de Lisboa
Faculdade de Ciências Sociais, Educação e Administração
Departamento de Ciência Política, Segurança e Relações Internacionais

Lisboa
2023

UNIVERSIDADE LUSÓFONA

LILIAN DILL DONATI GODINHO

CIBERTERRORISMO: A NOVA GUERRA FRIA?

Dissertação defendida em provas públicas para obtenção do grau de mestre no curso de Mestrado em Diplomacia e Relações Internacionais, conferido pela Universidade Lusófona – Centro Universitário de Lisboa, no dia 02 de maio de 2023, perante o júri, nomeado pelo Despacho de Nomeação Nº 203/2023, de 16 de março de 2023, com a seguinte composição:

Presidente: Prof. Doutor Vasco Rato
Arguente: Prof. Doutor Luís Bernardino
Orientador: Prof. Doutor José Filipe Pinto

Universidade Lusófona – Centro Universitário de Lisboa
Faculdade de Ciências Sociais, Educação e Administração
Departamento de Ciência Política, Segurança e Relações Internacionais

Lisboa
2023

EPÍGRAFE

A roda, o mundo em mudança, está sempre a girar, mas o eixo, que a acompanha, não muda. E o eixo são esses valores.

Adriano Moreira

DEDICATÓRIA

Dedico esta dissertação primeiramente aos meus queridos pais, que me transmitiram o gosto pelos estudos e, que apesar de não estarem mais entre nós, foram e sempre serão o meu maior exemplo e a minha grande fonte de inspiração.

Dedico especialmente ao meu marido, por todo seu amor, cuidado e carinho, por ter me incentivado e me apoiado incondicionalmente ao longo de tantos anos, pela sua convicção no meu potencial e por me fazer acreditar que nenhum desafio é grande demais quando se tem um sonho.

E, por último, dedico principalmente aos meus filhos por serem a minha razão de viver e de sonhar.

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer ao meu orientador Prof. Doutor José Filipe Pinto, a quem devo render todas as homenagens possíveis, por ter me orientado com excelência na execução da presente Dissertação de Mestrado. Apesar dos inúmeros compromissos acadêmicos sempre esteve disponível para compartilhar da sua expressiva capacidade intelectual de forma enriquecedora, inspiradora e objetiva para a minha aprendizagem e investigação. O meu profundo agradecimento por acreditar sempre na minha capacidade e pelo apoio incondicional, mesmo nos momentos mais difíceis, ao longo desse trabalho.

À Lusófona de Lisboa e a todos os Professores do mestrado de Relações Internacionais e Diplomacia da Universidade, pelas aulas e pelo precioso conteúdo partilhado durante o curso, pela dedicação mesmo durante os meses mais complexos da pandemia da Covid 19, em que ambos, alunos e Professores, tiveram que revelar persistência e coragem para não se deixarem abater.

Ao Professor Dr. Antônio Rebelo de Sousa pelo interesse e por propiciar o encontro com a ilustríssima Sra. Dra. Maria Luiza Proença - Diretora Nacional Adjunta da Polícia Judiciária, que me recebeu todas as vezes com gentileza ímpar e me direcionou internamente aos maiores peritos da instituição nessa temática.

Endereço o meu agradecimento também ao Dr. João Paulo Ventura, Coordenador da Unidade Nacional de Contraterrorismo da PJ e integrante desde 1997 do Grupo de Terrorismo da União Europeia na altura em que contribuiu para a presente obra com sua experiência e valiosos conselhos. Atualmente é Conselheiro de Justiça e Assuntos Internos junto ao Conselho da União Europeia e oficial de ligação da PJ.

Uma palavra igualmente especial ao Prof. Dr. Rogério Bravo, Coordenador de Investigação Criminal da Unidade Nacional de Combate ao Cibercrime e Criminalidade Tecnológica da Polícia Judiciária e representante da PJ no Centro Nacional de CiberSegurança. Obrigada pelas informações compartilhadas.

Quero agradecer especialmente ao Dr. Paulo Sérgio Pagliusi, Ph.D., CISM, Capitão-de-Mar-e-Guerra (RM1-IM), Diretor da ISACA (Information Systems Audit and Control Association) e Chief Information Officer da Apex-Brasil. A você o meu muito obrigada por pelo contributo profissional ao longo dos últimos 17 anos, pelo apoio e inspiração.

Por fim, agradeço a todas as pessoas, que de forma direta ou indireta contribuíram para realização do meu trabalho, não seria possível relacioná-los todos aqui, por isso, em nome de todos, destaco e agradeço especialmente o amigo Harold Wellington.

RESUMO

Depois de encerrado o período da Guerra Fria entre Estados Unidos e a extinta União Soviética, época em que, segundo Raymond Aron, a "Paz era impossível e a guerra improvável", o mundo está a presenciar o surgimento de uma nova Guerra Fria em que o Ciberterrorismo desempenha o papel principal.

A presente dissertação entitulada "Ciberterrorismo: A Nova Guerra Fria", tem como objetivo principal elencar as modalidades de terrorismo, definir o conceito de ciberterrorismo e perceber se trata-se de um mito ou uma realidade.

Face ao objetivo principal, esta dissertação pretende responder as seguintes perguntas de partida:

- O que é ciberterrorismo?
- Qual a verdadeira dimensão da ameaça do ciberterrorismo?
- A guerra no domínio cibernético é a nova Guerra Fria?

De forma a encontrar as respostas para as questões, no primeiro capítulo é feita uma contextualização teórica, abordando os conceitos operacionais, designadamente o terrorismo, as modalidades do terrorismo, o ciberterrorismo, o contra-terrorismo e o anti-terrorismo. No segundo capítulo, será analisada a evolução do ciberterrorismo, serão identificados os principais atores e relacionados alguns *cases* emblemáticos. E, finalmente, o terceiro capítulo analisa a nova guerra fria, no ambiente cibernético, travada entre a Rússia e Ucrânia no período entre 2013 e 2022.

Quanto à metodologia, utiliza-se à qualitativa, através de consulta de acervo publicado.

Palavras-Chave: Ciberterrorismo, Terrorismo, Guerra Híbrida, Nova Guerra Fria, Nova Ordem Mundial

ABSTRACT

After the end of the Cold War period between the United States and the extinct Soviet Union, a time when, according to Raymond Aron, "Peace was impossible and war improbable", the world is witnessing the emergence of a new Cold War in which Cyberterrorism plays the leading role.

The present dissertation entitled "Cyberterrorism: The New Cold War", has as main objective to list the modalities of terrorism, define the concept of cyberterrorism and understand if it is a myth or a reality.

In view of the main objective, this dissertation intends to answer the following starting questions:

- What is cyberterrorism?
- What is the true dimension of the cyberterrorism threat?
- Is the cyber warfare the new Cold War?

In order to find the answers to the questions, in the first chapter a theoretical contextualization is made, approaching the operational concepts, namely terrorism, modalities of terrorism, cyberterrorism, counter-terrorism and anti-terrorism. In the second chapter, the evolution of cyberterrorism will be analyzed, the main actors will be identified and some emblematic cases will be listed. And finally, the third chapter analyzes the new cold war, in the cybernetic environment, fought between Russia and Ukraine in the period between 2013 and 2022.

As for the methodology, the qualitative method is used, through consultation of published collections.

Keywords: Terrorism, Cyberterrorism, Hybrid War, New Cold War, New World Order

LISTA DE SIGLAS

ARPA	Advanced Research and Projects Agency
CEO	Chief Executive Officer
CERT	Community Emergency Response Team
CISA	Cybersecurity and Infrastructure Agency
CNCS	Centro Nacional de Cibersegurança
CSIRT	Computer Security Incident Response Team
DDos	Distributed denial-of-service
DNS	Domain Name System
DHS	Department of Homeland Security
DPRK	República Popular Democrática da Coreia
EM	Estados-Membros
ENISA	Agência Europeia para a Segurança das Redes e da Informação
ESI	Estudos Segurança Internacional
EUROPOL	Agência da União Europeia para a Cooperação Policial
FBI	Federal Bureau of Investigation
FSB	Serviço Federal de Segurança da Federação Russa
GDPR	General Data Protection Regulation
GOP	The Guardians of Peace
GWOT	Global War on Terrorism
IA	Inteligência Artificial
ICE	Infra-estruturas Críticas Europeias
IdC	Internet das Coisas
IoT	Internet of Things
INTCEN	Intelligence Analysis Centre
INTERPOL	International Criminal Police Organization
IRA	Exército Republicano Irlandês
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NED	National Endowment for Democracy
NSA	National Security Agency

OCDE	Organização para a Cooperação e Desenvolvimento Económico
OLP	Organização para a Libertação da Palestina
OMC	Organização Mundial do Comércio
ONU	Organização das Nações Unidas
PCC	Partido Comunista Chinês
PESC	Política Externa e de Segurança Comum
PNUD	Programa das Nações Unidas para o Desenvolvimento
RAF	Facção do Exército Vermelho
RI	Relações Internacionais
STRATCOM	Strategic Command
TIC	Tecnologias de Informação e Comunicação
UCA	A Aliança Cibernética Ucraniana
UE	União Europeia
URSS	União das Repúblicas Socialistas Soviéticas

ÍNDICE

Índice de Figuras

INTRODUÇÃO

Na conjuntura atual, o Mundo vive em conflito porque "o modelo das soberanias está em crise, posto em causa pelo que já se chama a pós-modernidade, rodeado pela ameaça das novas formas de guerra entre culturas que se enfrentam, tudo fazendo emergir uma busca de poder que reorganize a nova hierarquia, impedindo a paz" (Moreira, 2019, p.13). Uma realidade que, apesar de assumir algumas características novas, remete para a conjuntura saída da II Guerra Mundial.

De forma a fazer um breve paralelo entre a época atual e a época em que, segundo Raymond Aron, a paz era impossível e a guerra era improvável, o período da Guerra Fria entre os Estados Unidos da América (EUA) e a extinta União das Repúblicas Socialistas Soviéticas (URSS), assim como mencionado por MacMahon, "escrever uma história compacta do conflito que dominou e em grande parte definiu as relações internacionais por quase meio século revelou-se uma tarefa ao mesmo tempo desafiadora, emocionante e destemida"(2012, p. 7).

É de se observar que, de acordo com Chaves & Arguelhes (2014, p. 137), a Guerra Fria já foi conceituada de inúmeras formas com múltiplos significados, "desde o Juízo Final, como o foi, marcadamente, de 1950 a 1962, até certo tempo mais ordenado e previsível, recordado quase que com alguma nostalgia por determinados autores e atores internacionais do Pós-Guerra Fria". A questão posta era: como conter uma ameaça que era não apenas proveniente de um Estado, de um bloco, mas também uma ideiologia? Nesse contexto, houve uma bipolarização generalizada do mundo, e proveniente dessa bipolarização deu-se a corrida aos armamentos e a divisão do mundo em duas forças. No âmbito dessa temática, Moreira ressalta que deve-se então neste momento definir o que é esse fenômeno bipolar e nesse sentido, "O bipolarismo é um modelo de referência em cada conflito concreto, entre dois países, dois espaços ou dois blocos" (1997, p. 47).

Na visão de Buzan & Hansen (2010, pp. 156-160); "o fim da Guerra Fria potenciou a emergência de uma nova tendência nos estudos de segurança, a favor do alargamento e aprofundamento do seu significado". Este estudo ganhou ainda maior relevância devido ao surgimento de novas ameaças. Na verdade ,"a ameaça nuclear e de confronto entre superpotências em lugar a uma miríade de novas ameaças, muito embora nenhuma pudesse ascender à categoria de meta-evento ou de crise existencial

suprema". Assim, após a Guerra Fria, a maioria dos especialistas em segurança voltou o foco para a expansão das "novas ameaças" - ameaças essas que também incluíam a proliferação nuclear, armas químicas de destruição em massa, o crime organizado e o terrorismo. Dentro desse contexto, Buzan (2006, p. 2) também deixa claro que os Estados substituíram "o antigo sistema de ameaças da Guerra Fria por uma securitização quotidiana de ameaças, num período que é de "guerra contra o terrorismo".

Em se tratando de uma temática complexa, extensa e abrangente que pode se referir a uma tática, um ato anarquista, criminoso, com motivações políticas, religiosas ou ideológicas, existem inúmeras definições para a palavra Terrorismo e, trata-se de um "fenômeno quase tão antigo como o homem, embora ao longo da História tenha conhecido múltiplas facetas" (Pinto, 2018, p. 11). É de registrar que a palavra terrorismo vem do Reino do Terror incorrido por Robespierre durante a Revolução Francesa, no final do século XVIII, uma vez que naquela época, o termo se referia às ações brutais do Estado contra seus inimigos políticos.

O terrorismo contemporâneo, mais especificamente a partir de 2001, ano em que a Al Qaeda orquestrou os ataques aos Estados Unidos, o 11 de Setembro de 2001, influenciou os modelos de segurança, no sentido da compreensão da ameaça focada na Segurança Nacional dos Estados na guerra contra o terrorismo. Buzan & Hansen (2010) em *The Evolution of International Security Studies* contribuíram grandemente para a compreensão do conceito de segurança no período pós-11 de Setembro e nesse livro discutem a continuidade dos elementos securitários tradicionais existentes na época e a necessidade da expansão do conceito de segurança internacional na guerra contra o terrorismo.

O terrorismo não é apenas praticado por pessoas, grupos, mas também por Estados. Segundo Chaliand, o terror é usado como um "modo de governar, permitindo que o poder estabelecido, por meio de medidas extremas e do medo coletivo, acabe com aqueles que resistem a ele"[1]. Um exemplo disso é a realidade que rege o atual sistema de governo chinês, através do programa de crédito social que "para além da sua componente de controle e vigilância estatal, tem uma dimensão comercial. Virtualmente sem limites, os dados são recolhidos sobre todos os aspectos da vida financeira e das preferências de consumo dos cidadãos, dados que, aliás, são partilhados com o serviço

[1] Encyclopedia Universalis. Disponível em: http://www.universalis.fr/encyclopedie/terrorisme/. Recuperado em 20 de Janeiro de 2022.

de vigilância do Estado. Esta informação constitui um recurso inimaginável para aumentar a competitividade das empresas" (Rato, 2020, p. 143). É importante frisar que a China não somente tem o controle da informação e de todos os dados da população e das empresas estatais, como vem caminhando a passos largos rumo ao domínio da guerra tecno-comercial com os Estados Unidos, liderando dois setores tecnológicos importantíssimos, que são a Inteligência Artificial (AI) e o sistema 5G, pois, o 5G associado à Inteligência Artificial irá revolucionar as economias. Será uma revolução nos processos produtivos.

Contudo, a conceituação de Terrorismo de Estado, no âmbito das Relações Internacionais, das organizações intergovernamentais ou empresariais, não é tarefa simples. Confrontar este aspecto do "terrorismo de Estado", indubitavelmente leva a debates intermináveis e intensos, principalmente no que se refere ao Ciberterrorismo, cuja ação dificilmente se consegue atribuir a um Estado. Nesse sentido, os Estados que viessem a causar danos colaterais incomensuráveis no espaço virtual, poderiam ser caracterizados como "Estados Terroristas", que violam leis internacionais.

Parece, assim, possível dizer que, o mundo está a assistir ao surgimento de uma revisitação do clima de Guerra Fria em que o Ciberterrorismo desempenha o papel principal. Moreira (2019, p. 12) afirma que "hoje o problema essencial é assumir que o «poder de destruir o planeta» está pendente, como talvez repetisse Bismark, de uma simples leviandade".

O Ciberterrorismo e a sua real ameaça no cenário atual constituem o cerne desta dissertação, entitulada «Ciberterrorismo: A Nova Guerra Fria?», tem como objetivo principal elencar as modalidades de terrorismo, definir o conceito de ciberterrorismo e perceber se se trata de um mito ou de uma realidade passível de configurar uma nova Guerra Fria.

Face ao objetivo principal, esta dissertação pretende responder às seguintes perguntas de partida:

- O que é ciberterrorismo?

- Qual a verdadeira dimensão da ameaça do ciberterrorismo?

- A guerra no domínio cibernético é a nova Guerra Fria?

De forma a encontrar as respostas para as questões, no primeiro capítulo faz uma contextualização teórica, abordando os conceitos operacionais, designadamente o ciberterrorismo, o ciber-crime e a ciber-guerra. O segundo capítulo, analisa a evolução

do ciberterrorismo, identifica os principais atores e cita alguns casos mais emblemáticos, dentre inúmeros outros, que apesar de terem resultado em perdas financeiras bilionárias, não são objeto deste trabalho, assim como também não é o objetivo dessa dissertação especificar tecnicamente a abordagem utilizada em cada ciberataque.

Finalmente, o terceiro capítulo analisa a nova guerra fria, no ambiente cibernético, travada entre a Rússia e Ucrânia, no período entre os anos de 2013 a 2022.

Para encontrar a resposta às perguntas de partida e atingir os objetivos definidos nesta dissertação, perceber se o Ciberterrorismo trata-se de uma ameaça a ser realmente configurada como a "Nova Guerra Fria" e sua verdadeira dimensão na construção de uma nova Ordem Mundial, privilegia-se a metodologia qualitativa, através de consulta de acervo publicado, de relatórios e de documentos oficiais.

Capítulo I

1. Enquadramento Teórico

1.1 Terrorismo Global

O terrorismo existe desde os primórdios da humanidade, é intrínseco ao ser humano e é tão complexo e heterogêneo que torna a tarefa de conceituação particularmente obscura diante da ausência de consensualidade, não somente entre autores, mas entre Instituições e Estados. De acordo com Pierre-Marie Dupuy, existem mais de cem possíveis definições de terrorismo[2].

De assinalar que a palavra terrorismo vem do período do Terror incorrido por Robespierre durante a Revolução Francesa, no final do século XVIII, uma vez que naquela época, o termo se referia às ações brutais do Estado contra seus inimigos políticos. Para a temática em estudo interessa dizer que todo ato terrorista continua a ter uma característica comum, o fato de causar o terror na população civil.

De acordo com Moreira (2001, p. 190) "o terror é um procedimento que não exige excessivos meios materiais e humanos, está ao alcance de grupos restritos e tem o campo de ação quase ilimitado".

Já para Baêna (2006, pp.120-126) o conceito de terrorismo é definido através de seis premissas básicas:

> 1. "O terrorismo é o uso previsto de uma violência convertida de um crime ou ameaça de violência; 2. Terrorismo é uma seleção deliberada de uma tática para efetuar mudanças; 3. Terrorismo é atingir pessoas inocentes, incluindo militares; 4. Terrorismo é o uso de atos simbólicos para atrair a mídia e obter larga audiência; 5. Terrorismo é uma forma ilegítima de combate, mesmo em guerra; 6. O terrorismo nunca é justificado".

Butler (2002, p.4) por sua vez, sugeriu apenas uma tipologia de terrorismo com duas categorias: instrumental e retributivo. A exemplo do primeiro, cita o IRA (O Exército Republicano Irlandês) e a OLP (A Organização para a Libertação

[2] De acordo com Pierre-Marie Dupuy, existem pelo menos 109 possíveis definições de terrorismo. [DUPUY, Pierre-Marie (2004). "State Sponsors of Terrorism: Issus of Responsibility", in: BIANCHI, Andrea (Ed.), Enforcing International Law Norms against Terrorism. Portland: Hart; p. 5].

da Palestina), consideradas grupos de terrorismo político que praticam atos a fim de conseguirem alcançar um objetivo e uma vez alcançados, não recorrem a mais atos.

Quanto ao terrorismo retributivo, a ato em si visa a destruição do inimigo. Nessa categoria Butler inclui os grupos supremacistas brancos da América e os terroristas radicais islâmicos.

Várias abordagens sobre o terrorismo poderiam ser relacionadas nessa dissertação, entretanto foi selecionado o denominado terrorismo global, que surgiu a partir do sec. XIX, e ao longo desse capítulo serão elencadas suas diferentes facetas, tais como: o terrorismo anarquista, anti-colonialista, contestatário de esquerda e religioso, conforme a classificação feita por David Rapoport: as quatro ondas.

O terrorismo anarquista foi a fase em que o ato terrorista era perpetrado contra quem detinha o poder. É inevitável não citar três exemplos históricos emblemáticos, o assassinato do rei D. Carlos I de Portugal e do Príncipe herdeiro D. Luís Filipe em 1 de Fevereiro de 1908, perpetrado por anarquistas "os conjurados". Assim como o rei de Itália, Humberto I, morto a 29 de Julho de 1900 pelo anarquista Caetano Bresci. E o assassinato do Arquiduque Francisco Fernando do Império Austro-Húngaro e a sua mulher em 28 de Junho de 1914 em Sarajevo, pelo grupo nacionalista sérvio "Mão Negra", evento este considerado o estopim para I Guerra Mundial.

O terrorismo anti-colonialista, ocorreu no período que se estendeu de 1920 a 1960, e está ligado com o desmantelamento dos impérios coloniais europeus, momento configurado por uma fase de luta das colônias para ganhar a independência, através de atos perpetrados contra o Estado e não as figuras políticas específicas e visava criar novos Estados. A ideologia contra a prática do colonialismo remonta ao início do século XX, período em que a questão da autonomia nacional africana foi levantada vagamente pela primeira vez[3].

O terrorismo radical, classificado como a 3ª. onda, vai de 1960 a 1990 e possui elementos de extrema esquerda. Os grupos terroristas agora passam a ter uma vertente transnacional e passam a se intercomunicar. O símbolo da luta ideológica da nova esquerda foi a resistência dos vietcongues na guerra do Vietnã contra os Estados Unidos da América. Esse modelo heroico foi sucedido pela OLP (Organização pela Libertação da Palestina) cujo marco foi o atentado contra os atletas olímpicos israelenses nas

[3] 3 Cf. Pedro Pezarat Correia, «Descolonização» in Do Marcelismo ao Fim do Império, Lisboa, Editorial Notícias, 1999, p. 112.

Olimpíadas de Munique em 1972 e teve enorme repercussão internacional chamando a atenção para a causa palestina. O atentado terrorista ocorreu durante um evento coberto pela mídia internacional, para chamar a atenção do mundo, em um território que não estava envolvido em disputa, ou seja, passam a não haver fronteiras nem limites territoriais para a consumação dos atos terroristas. A exemplo disso, há dois fatos históricos importantes a serem mencionados, o primeiro refere-se ao sequestro do ex premiê italiano Aldo Moro, em maio de 1978, mantido em cativeiro por 55 dias e que culminou com seu assassinato, tendo sido encontrado morto na bagageira de um veículo, fato que marcou o ápice do movimento das Brigadas Vermelhas na Itália.

Na Alemanha, a Facção do Exército Vermelho (RAF), grupo fundado por Andreas Baader ao qual pertenceu também a ativista de esquerda Ulrike Meinhof, em cujas raízes estava o movimento estudantil e a oposição à guerra do Vietnam, anunciou a sua dissolução em abril de 1998, em carta enviada à agência Reuters. Em três décadas de existência, "a organização assassinou pelos menos 50 pessoas entre militares americanos, políticos e empresários"[4].

Na França os alvos eram, principalmente, os líderes políticos e os empresários de destaque. E, após os assassinatos do general René Audran, em 1985, e do presidente da Renault, Georges Besse, em 1986, o Estado francês agiu com rigor, tendo êxito ao prender os fundadores do grupo, Jean-Marc Rouillan, Nathalie Ménigon e Georges Cipriani, o que levou à dissolução do grupo.

Os extremistas de esquerda, assim como na Itália, na Alemanha e na França, tinham o mesmo princípio ideológico, a criação de uma "frente antiimperialista européia", segundo Rolf Tophoven, diretor do Instituto de Pesquisa sobre Terrorismo e Política de Segurança, "a Fração do Exército Vermelho (RAF), as Brigadas Vermelhas e a Action Directe respectivamente tinham em comum a meta de uma revolução social"[5]. Apesar das similaridades dos meios empregados através da violência, esses grupos nunca formaram uma rede de cooperação internacional como se vê atualmente empregada pelos grupos terroristas islâmicos.

[4] Beck, J. (s.d.): 1998: Grupo terrorista alemão RAF anuncia dissolução. Recuperado de: https://www.dw.com/pt-br/1998-grupo-terrorista-alem%C3%A3o-raf-anuncia-dissolu%C3%A7%C3%A3o/a-306977. (Em : 11/07/2022)

[5] Rottscheidt, I. (2007): Movimentos revolucionários. Recuperado de: https://www.dw.com/pt-br/o-que-restou-do-terrorismo-de-esquerda-na-europa/a-2347037. (Em: 11/07/2022)

No que compete à definição da Comissão Europeia contra o Racismo e o Terrorismo (ECRI) a radicalização refere-se ao processo pelo qual alguém adota ou incorpora valores políticos, religiosos ou sociais incompatíveis com os valores que regem as democracias[6].

Similarmente Borum (2017, pag. 18) entende que o processo de radicalização do indivíduo ou grupo refere-se à adoção de convicções políticas, sociais e/ou religiosas e as pretensões extremistas que rejeitam a ordem democrática convencionada ou os ideais que predominam num Estado. A complexidade quanto à conceituação em relação ao fenômeno do terrorismo já foi mencionada no início desse capítulo, da mesma forma nas palavras de Ventura & Gomes (2020, p. 64) "são sobejamente conhecidas diversas noções ou conceitos de radicalização, mas nenhuma delas é universalmente aceite".

A designada 4ª. vaga que se iniciou em meados de 1990, e se mantém até hoje, ganhou o componente religioso que busca a criação de um Estado cujo propósito principal é alicerçado na religião e na lei da sharia. Alguns autores, como Phillips (2010, p. 139), afirmam que um ingrediente fundamental dessa vaga é a "contestação de governos autocráticos no mundo muçulmano nos anos 70 e 80, que se aliaram aos Estados Unidos para garantir sua sobrevivência política".

Para Hoffman (2006) "a violência é um ato sacramental ou dever divino executado em resposta direta a um imperativo ou uma procura teológica"[7].

O terrorismo dito religioso, entretanto não está restrito ao fundamentalismo islâmico, apesar da sua indubitável proeminência. Rapoport (2002, p. 8) afirma por sua vez que: "o terrorismo islamista é hoje um fenômeno criminal global que exige resposta concertada entre os Estados à escala planetária". Os fundamentalistas islâmicos visam impor um califado global e destriur os regimes não islâmicos, varrendo os ocidentais e não crentes de territórios sob domínio islâmico. De acordo com Abul Ala Maududi (2006, p.5) a jihad tem uma razão de ser intrínseca, uma vez que o Islão não significa uma religião e ser muçulmano não representa um título. De acordo com Pinto (2018, p.19) a jihad refere-se sim à luta revolucionária e ao esforço máximo que o Partido Islâmico faz para atingir o objetivo de alterar a ordem social em todo Mundo de maneira a reorganizá-la de acordo com os seus princípios e ideais.

[6] European Comission against Racism and Intolerance (2016, pag. 27)
[7] Hoffman, B. (2006). Inside Terrorism, New York: Columbia Unibersity Press, p. 88

Padahzur & Martim (2017, p. 340), assim como a maioria dos autores investigados ao longo desse trabalho, reiteram que os atentados de 11 de setembro de 2001 foram os mais mortíferos e demolidores ataques terroristas que a História registrou, dividido em várias frentes, porém atingindo um único país. Esse episódio levou à atual sensação de insegurança individual e coletiva. Realidade essa que muito satisfaz aos terroristas, já que o sentimento de que nenhum lugar é totalmente seguro para a sociedade civil é a decorrência tencionada pelos terroristas, de acordo com Bianchi (2004, p vi).

Como já foi dito anteriormente, o terrorismo global é um fenômeno que vem se transformando ao longo do tempo, alguns autores afirmam que depois dos atentados de 11 de Setembro de 2001, as organizações islâmicas têm encorajado cada vez mais os ataques realizados por lobos solitários contra alvos que eles reconhecem como sendo inimigos, com grande destaque no Ocidente. Essa estratégia é muito utilizada pelo grupo terrorista Al Qaeda, com o propósito de utilizar indivíduos ou pequenas células terroristas, alheias umas das outras para atacar diversos alvos civis, "contra interesses ocidentais e, gradualmente, transformariam o fenômeno em algo que poderia tornar-se um movimento em massa, coordenado e dirigido" (Lia, 2018, pp. 18-19).

Em 2010, o canal de comunicação social da Al Qaeda, divulgou um vídeo em inglês com o título sugestivo *'A Call to Arm'*, através do qual elogiava a ação de lobos solitários e incentivava todos os jihadistas que vivessem nos Estados Unidos, Israel e Reino Unidos a seguir o mesmo exemplo contra os incrédulos, buscando alvos que poderiam representar graves prejuízos econômicos para estes países, como os ataques de 11 de Setembro de 2001, para provar que tais ataques não precisam o emprego de armas convencionais, necessariamente, como descreveu Weimann (2012, pp. 80-81). A Al Qaeda incentivava também indivíduos a cometer ataques terroristas fora de qualquer cadeia de comando terrorista, por iniciativa própria, sem esperar instruções de forma a enfraquecer a potência ocidental a partir de dentro.

Resumidamente, o terrorismo islâmico age em nome da religião, não obstante do cunho político, tornou-se um fenômeno global, que possui não apenas um Estado por trás, mas múltiplos atores que têm a capacidade de causar profusos ataques, orquestrados ou não, em diferentes regiões do globo, com elevado grau de destruição, causando enormes prejuízos e perdas de vidas.

Na atualidade, o terrorismo global refere-se ao terrorismo transnacional por meio do qual atores violentos não estatais atuam em vários territórios, cujos atos são difíceis de prever e monitorar, e cuja atividade foi infinitamente facilitada com a globalização e a internet, alargando o campo de atuação terrorista, que passou a ser orquestrado de diversas formas, no ciberespaço.

Os meios que podem ser utilizados pelo terrorismo estão em evolução constante e, na atualidade, são[8]:

- Convencionais: através da utilização de armas de fogo e explosivos,

- Biológicos: através do uso de armas biológicas (ex: criação de vírus),

- Químicos: através do uso de armas químicas (ex: gases tóxicos),

- Radiológicos: através do uso de fontes istotópicas,

- Nucleares: através da transferência de artefatos de uso militar de países simpáticos à causa terrorista, como o Irã e o Paquistão, seja através da aquisição de armas nucleares, seja através da aquisição no mercado negro de urânio altamente enriquecido (um dos combustíveis dessas armas), seja através do tráfico de material nuclear ou roubo de armas nucleares de países como Rússia, Coreia do Norte e Paquistão, cujos programas de fiscalização internacional são insuficientes ou inexistentes.

- Cibernéticos: através de ataques a sistemas de informação governamentais ou privados, o qual será abordado mais detalhadamente nessa tese.

1.2 Conceitos operacionais de Ciberterrorismo, Cibecrime e Ciberguerra

De acordo com Lara & Al (2014, p. 25) "para que um ataque possa ser qualificado como ciberterrorista, este deve resultar da violência contra pessoas ou bens ou, pelo menos, causar dano suficiente para gerar medo". Contudo, os mesmos autores ratificam quão fundamental é distinguir o ciberterrorismo, do cibercrime e da ciberguerra já que "a distinção não resulta do meio utilizado mas da finalidade principal da ação". O cibercrime tem como finalidade uma vantagem "patrimonial, por meios ilícitos, direta ou indiretamente. A ciberguerra constitui a "nova forma de terrorismo de

[8]Costa, T.(s.d.) identifica seis meios utilizados pelo terrorismo. Recuperado de. Disponível no sítio: https://www.ceped.ufsc.br/wp-content/uploads/2010/01/TADEU-DE-LERY-COSTA-CONTRATERRORISMO-NO-AMBITO-DA-INTELIGENCIA.pdf (em 23/04/2022)

Estado". Dada a diversidade e extensão do tema esta dissertação procurará evidenciar as questões relativas mais especificamente ao ciberterrorismo.

Segundo Rogério Bravo, autor constantemente citado internacionalmente e referência na matéria, a revolução tecnológica e o exponencial desenvolvimento de meios de comunicação e informação de base *ciber* criaram novas possibilidades, transformaram completamente as "práticas e dinâmicas da radicalização político-ideológica", assim como a materialização do "chamado extremismo político criminal" e por consequência também as "possibilidades de resposta das autoridades, no plano da reação e prevenção" (Bravo, 2011, pp. 174-200). No que se refere à Lei Portuguesa contra o Terrorismo Lei nº52/2003[9]- Pedro Freitas afirma que "para a questão de saber se afinal o ciberterrorismo encontra amparo na lei portuguesa, a resposta é afirmativa"[10].

De acordo com Denning (2000) "o ciberterrorismo é a convergência entre o ciberespaço e o terrorismo. São ataques ilegais contra os computadores, redes e as informações neles armazenadas, efetuados para intimidar ou coagir um Governo ou o seu povo, em prol de objetivos políticos ou sociais", diferente do conceito de *hackitivismo*, também já apresentado pela mesma autora (199, p. 241); que significa a interseção entre o *hacking* e o ativismo.

De assinalar que Ventura & Carvalho b (2020, p. 165) mencionam que o desenvolvimento do ambiente cyber "também não escapou à atenção dos intérpretes do terrorismo". E sobre essa questão, Nunes (2015, p. 142) afina pelo mesmo diapasão ao afirmar que "os ciberataques instrumentais perpetrados por extremistas, por lobos solitários e por simpatizantes ou agentes do terrorismo são bem mais verossímeis e de resto já ocorreram".

Para Wiemann (2004, pp. 1-4) o Ciberespaço é o ambiente ideal para os criminosos praticarem seus delitos, os cibercrimes, de forma anônima que proporciona a possibilidade de impor prejuízos transversais de acordo com a motivação conveniente a cada ator. Para além disso, o mesmo autor afirma também que o ciberterrorismo tem motivações políticas, visa graves danos e perdas, de natureza econômica e de vidas humanas. Através do ciberterrorismo é possível gerar graves perturbações junto às redes de infraestruturas críticas, como as redes de energia, de abastecimento de água, em

[9] Diário da República Eletrônico: Lei n.º 52/2003, de 22 de agosto. https://dre.pt/dre/detalhe/lei/52-2003-656128 (em: 22.06.2022).
[10] Freitas, P. (2022, pp. 115-130): Ciberterrorismo e a Lei de Combate ao Terrorismo. https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD161/NeDef161_6_PedroMiguelFreitas.pdf. (em: 22.06.2022).

sistemas de transporte aéreo e de controle de tráfego, em sistemas hospitalares, em mercados financeiros, entre tantos outros assentes nos modernos sistemas de tecnologia da informação e processamento da informação, altamente complexos e vulneráveis. Vivemos numa Era em que a informação é tudo e, nesse sentido a capacidade de cada Estado de processar, armazenar difundir e salvaguardar as suas informações é sinônimo de poder.

O ciberterrorismo é uma revisitação da época em que o mundo vivia uma Guerra Fria porque é a primeira estratégia ofensiva sem o uso de recursos tradicionais de guerra e corresponde por isso, a uma nova dimensão do poder nas Relações Internacionais e que irá condicionar a construção de uma Nova Ordem Mundial. A resposta do Ocidente ao ciberterrorismo baseia-se numa estratégia de defesa, já que a opinião pública dos Estados democráticos jamais aceitaria que o ciberterrorismo fosse combatido na mesma moeda. Nesse sentido, o Ocidente se organiza de forma a criar órgãos e mecanismos que falem entre si e permitam desmantelar as redes internacionais de ciberterrorismo, que por sua vez praticam cada vez mais ataques mais ofensivos.

É importante esclarecer que o Ciberterrorismo é uma variante do terrorismo relativamente recente e está ligado ao conceito de *Sharp-Power*[11] criado em 2017. O Sharp-Power é uma estratégia intermédia entre o *Soft-Power*[12] e o *Hard-Power*[13]. Através da manipulação da informação é possível criar junto à opinião pública um ambiente favorável ou desfavorável para quem interessar.

[11] O National Endowment for Democracy (NED) popularizou em 2017 o termo "Sharp-Power"; apareceu em um artigo na revista Foreign Affairs descrevendo políticas agressivas e subversivas empregadas por governos autoritários como uma projeção do poder do Estado em países democráticos, políticas que não podem ser descritas como hard power ou soft power. O artigo do NED cita especificamente a RT News Network, financiada pelo estado russo, e as parcerias educacionais do Instituto Confúcio, patrocinado pelo estado chinês, como exemplos de Sharp Power. De acordo com o NED, os estados autocráticos "não estão necessariamente buscando" ganhar corações e mentes "(o quadro comum de referência para os esforços de soft power), mas certamente procuram manipular seus públicos-alvo distorcendo as informações que os chegam.

[12] É uma expressão usada na teoria das relações internacionais para descrever a habilidade de um corpo político – um Estado, por exemplo — para influenciar indiretamente o comportamento ou interesses de outros corpos políticos por meios culturais ou ideológicos. O termo foi usado pela primeira vez pelo professor de Harvard, Joseph Nye, no final dos anos 1980. Ele desenvolveu o conceito em seu livro de 2004, *Soft Power: The Means to Success in World Politics* . A expressão *soft power* entrou, desde então, no discurso político como uma maneira de distinguir os efeitos sutis de culturas, valores e ideias no comportamento de outros.

[13] É um conceito usado para designar a capacidade de um corpo político (geralmente, um Estado) de influenciar ou exercer poder sobre o comportamento de outro, mediante o emprego de recursos militares ou econômicos. Isso pode ser feito com o uso de diplomacia coerciva, do poder militar, da guerra ou formação de aliança mediante ameaças e força, coerção, intimidação e proteção. O poder econômico também pode ser usado alternativamente, sob a forma de ajuda financeira, subornos e sanções econômicas para induzir e coagir.

Convém dizer que, o termo *Soft-Power* foi utilizado pela primeira vez pelo professor de Harvard Joseph Nye, no final dos anos 1980. O autor lançou em 2004 seu livro *Soft Power: The Means to Success in World Politics,* em que se refere à estratégia de conquista do coração e mente, sem o uso da coerção, persuasão e força. É uma relação de ganho-ganha para todos os Estados envolvidos no processo. Trata-se do poder de convencimento de forma pacífica. Já o termo *Hard-Power* refere-se ao extremo oposto, ou seja, o uso ou ameaça do uso da força militar para alcançar os objetivos, através dos recursos tradicionais de guerra, a subida aos extremos ou o recurso ao eixo polemológico das Relações Internacionais.

O *Sharp-Power* é a promovido através do controle da informação, da sua manipulação interna e externamente de forma a torná-la coercitiva e nesse contexto a vontade passa a ser direcionada para atingir determinado propósito que está condicionado à escolha do outro. O *Sharp Power* está relacionado com a habilidade de um governo influenciar e direcionar o pensamento coletivo, da opinião pública seja internamente, controlando a opinião pública, ou de um outro Estado, com o objetivo de manipular e mudar o seu comportamento de forma a condicionar, controlar, interferir, desestabilizar ou destruir o sistema governamental desse país sem fazer uma ameaça aberta e direta. Assente na natureza danosa do *Sharp-Power* está inserido o ciberterrorismo que parte de regimes autocráticos e não democráticos, e todavia não é alvo de retaliação na mesma proporção, ou seja, não se responde ao terror com terror. Trata-se da estratégia adotada por regimes autocráticos para manipular os ambientes político e informacional dos países-alvo.

Joseph S. Nye, Jr.(2018) afirmou que a China tem usado o *Sharp-Power* como meio de obter os resultados desejados quanto à sua política externa de não interferência para aumentar a influência em vários países. "*Whereas soft Power harnesses the allure of culture and values to augment a country´s strength, sharp power helps authoritarian regimes compel behavior at home and manipulate opinion abroad*"[14]. A China tem usando o Sharp-Power para promover os seus interesses, manipulando o cenário político internacional, através de pretensas atividades, tais como: ajuda econômica transnacional, atividades culturais, intercâmbio de estudantes, programas educacionais entre outros, influenciando a seu favor a mídia e opinião pública. Além da criação do

[14] Project Syndicate: The Worlds Opinion Page, Recuperado de: https://www.project-syndicate.org/commentary/china-soft-and-sharp-power-by-joseph-s--nye-2018-01 (em 12/12/2021)

audacioso projeto de infraestruturas da Nova Rota da Seda, um programa que envolve trilhões de dólares em endividamento de muitos países em troca de investimento chinês em infraestruturas e desenvolvimento, para construção de estradas, portos, centrais elétricas, no setor de telecomunicações, dentre outros (Lew & Roughead, 2021).

De acordo com o relatório divulgado em 2018 pelo Centro Nacional de Contrainteligência e Segurança sobre Espionagem Econômica Estrangeira no Ciberespaço, a China continua a usar "espionagem cibernética para fortalecer seus objetivos estratégicos de desenvolvimento"[15].

1.3 Antiterrorismo e Contraterrorismo

Na Arte da Guerra, Sun Tzu, já preconizava que "aquele que não conhece o inimigo e tampouco a si mesmo será invariavelmente derrotado em todos os confrontos" Sawyer (2010, p.40). Essa prática atualmente é chamada de Inteligência!

A circunstância primordial para o sucesso na implementação de quaisquer medidas de contraterrorismo e antiterrorismo são o fundamento num sólido sistema de inteligência. Todo conhecimento e informação pertinente e imprescindível é resultado de estudos e análises de diversas agências de inteligência internacionais que cooperam entre si num esforço internacional de combate ao terrorismo. A busca e a coleta multidisciplinares de informações que envolvem diversas áreas como a política, econômica, psicossocial, militar, cientifica e tecnológica, são indispensáveis na gestão das operações preventivas quanto nas repressivas, ou seja, antiterroristas e contraterroristas respectivamente.

Os Estados têm investido e concentrado imensos recursos e esforços em atividades de inteligência, cujo papel é propiciar a implentação de políticas e estratégias para dirimir as ameaças terroristas.

O antiterrorismo envolve as atividades de natureza defensiva que visam mitigar as vulnerabilidades de indivíduos e lugares de ataques terroristas. Nesse aspecto, as atividades e normas que regulam as operações desenvolvidas pelos órgãos de segurança tanto nos aeroportos, portos e fronteiras; a fiscalização exercida pelos órgãos de controle de migração; a segurança voltada para proteção dos serviços públicos

[15] Amaresh P. (2020, p.2): The Art of War- Chinas Sharp Power Strategy 2020. Recuperado de: https://www.academia.edu/search?q=The%20Art%20of%20War-%20Chinas%20Sharp%20Power%20Strategy%202020 (em 18/01/2022)

essenciais, bem como o patrulhamento das principais vias de transporte público e comunicações, todas estão enquadradas no conceito de antiterrorismo, e possuem caráter defensivo.

O contraterrorismo, por sua vez, envolve a implantação de medidas essencialmente ofensivas e tem como alvo as diversas organizações terroristas, com o objetivo de prevenir, dissuadir, ou retaliar atos terroristas. É voltado para as estratégias de dissuasão do inimigo para cometer atos terroristas. De acordo com o Departamento de Defesa dos Estados Unidos da América (2007)[16] a definição coincide com a mesma empregue pela NATO, assim como por outras agências militares, que descrevem o contraterrorismo como a operação que inclui medidas ofensivas para prevenir, deter e responder a atos terroristas. As operações realizadas por equipes altamente especializadas que visam a captura de membros de grupos terroristas, como também para libertar instalações ou reféns que estejam sob o domínio dessas organizações, são enquadradas como ações de caráter contraterroristas.

Segundo Jonathan Matusitz (2013, p. 415), as seis componentes principais do contraterrorismo são:

- Impedir simpatizantes de aderirem a grupos terroristas,
- Criar discórdia entre os grupos,
- Possibilitar dissidências,
- Reduzir o suporte aos grupos,
- Tornar os líderes menos legítimos,
- Proteger o público-alvo do objetivo do ataque terrorista.

Relativamente ao que se refere à (r)evolução da atividade de Inteligência nas últimas décadas, é impossível deixar de mencionar o Decreto de 26 de Outubro de 2001, assinado pelo presidente George W. Bush "*USA PATRIOT Act*" que permitiu após os atentados de 11 de setembro de 2001, entre várias medidas, que órgãos de segurança e de inteligência dos EUA intersectassem ligações telefônicas e e-mails de organizações e pessoas americanas ou estrangeiras, que pudessem estar envolvidas com o terrorismo, sem necessidade de qualquer autorização da Justiça[17].

[16] U.S. Department of Defense (2017). Joit Publicatiom 1-02 Department of Defense Dictionary of Military and Assoiated Terms. Arlington, VA: U.S. Department of Defense

[17] https://exame.com/mundo/o-que-mudou-depois-do-11-de-setembro-relembre-o-ataque-19-anos-depois/(em 22/06/2022)

Capítulo II

2. A Evolução do Ciberterrorismo

2.1 Os Principais Atores

De modo a remontar o cenário atual é imprescindível mencionar a importância dos trabalhos precursores de interceptação e desencriptação realizados durante a Segunda Guerra Mundial executados pelos britânicos, liderados pelo matemático Alan Turing, através da sua máquina Enigma, que permitiu através de milhares de combinações, decifrar as ordens encriptadas enviadas pelos alemães, o que viabilizou em grande parte a vitória dos aliados na grande guerra. No tempos atuais, com milhares de informações sensíveis e estratégicas armazenadas em computadores ligados em rede, a partir de momento em que o servidor estiver ligado à internet, o risco de ser invadido ou infectado é real.

A guerra cibernética desempenha um papel importante no mundo moderno e trata-se de uma atividade de suma importância, de modo que todas as potências militares mundiais já criaram unidades e agências especiais dedicadas a ela. A guerra cibernética envolve duas frentes importantes, a espionagem e a sabotagem, que vão desde a destruição de projetos e documentos até levar a cabo ações diretas contra infraestruturas controladas por computadores. As infraestruturas críticas de um país referem-se ao fornecimento, no meio físico ou digital, de serviços essenciais à sociedade que, caso sejam afetadas por um ataque cibernético, podem acarretar profundo impacto não somente na área de segurança do país alvo do ataque, como também para os segmentos político, financeiro, de energia, saúde, transportes, comunicações e nuclear entre outros.

Segundo a *Cybersecurity and Infrastructure Agency* (CISA)[18], agência americana responsável pela Segurança Cibernética e Infraestruturas que lidera o esforço nacional para compreender, gerir e reduzir os riscos cibernéticos, os sistemas críticos de um país estão classificados em dezesseis setores fundamentais, como demonstrado no quadro abaixo.

[18] Cybersecurity and Infrastructure Agency (CISA). Recuperado de: Fonte: https://www.cisa.gov/about-cisa (em 07/02/2022)

A agência tem a missão de proteger e defender as redes governamentais, através do trabalho em parceria com o Gabinete de Gestão e Orçamento Americano, visando assegurar que a informação atempada e acionável seja partilhada entre parceiros federais e não federais e do sector privado.

Figura 1 - Infraestruturas criticas de um país, segundo a CISA

Fonte: https://www.cisa.gov/about-cisa (Recuperado em 07.02.2022)

Nem todos os países possuem planos concretos e eficazes de segurança cibernética para proteger suas infraestruturas críticas e estão mais suscetíveis aos ataques. Por isso, é de suma importância que os governos e empresas invistam no desenvolvimento e implementação de estratégias que visem a restrição dos riscos para suas infraestruturas críticas.

Atualmente existem entre vinte a trinta países conhecidos por terem unidades de guerra cibernética qualificadas, além dos Estados Unidos e Rússia, que são os países com maior destaque. Não se sabe exatamente o total do montante que cada país dedica para desenvolvimento dessa área, mas são valores muito elevados que crescem a cada ano. Sabe-se, isso sim, que há países relativamente pequenos como Irão e Coreia do Norte que investem muito nesse tipo de atividade de forma a ganharem espaço na cena internacional. Nesse capítulo serão abordados alguns dos principais atores estaduais, entretanto, é importante frisar a relevância dos atores não estaduais nos ciberconflitos, especialmente nas situações em que estes são recrutados e coordenados por Estados, ainda que de forma oficiosa. Proliferam-se a cada minuto ataques cibernéticos liderados por grupos subnacionais, como nos casos do hacktivismo e cibercrimes, ou comandados por Estados, como a ciberespionagem e a sabotagem.

2.1.1 Os Estados Unidos da América

Segundo Clarke, R. & Knake, R. (2015) "Todo o fenômeno da guerra cibernética é de tal forma cercado de sigilo governamental que faz os tempos da Guerra Fria parecerem uma época de transparência e abertura". Trata-se atualmente da arma mais poderosa desejada por todos os exércitos do mundo. Nesse campo, os Estados Unidos foram os precursores, tendo criado, em 2009, o Comando Cibernético da Força Aérea dos Estados Unidos, responsável por proteger a rede de computadores militares dos Estados Unidos e subordinado ao Comando Estratégico dos Estados Unidos. De lembrar também que a própria Internet foi criada durante a Guerra Fria, no fim da década de 1960, também pelos Estados Unidos, pelo Departamento de Defesa para fins militares, mais especificamente pela Advanced Research and Projects Agency (Arpa). O projeto foi financiado pela NASA e pelo Pentágono e tinha objetivo primordial de criar uma rede que fosse capaz de armazenar dados e permitir a continuidade da comunicação mesmo em caso de um ataque nuclear[19]. Mais tarde, a possibilidade de usar a arma cibernética em guerras não foi subestimada e, em 1995, a Universidade de Defesa Nacional formava a primeira turma de oficiais treinados para conduzir campanhas de guerra cibernética.

Os Estados Unidos haviam criado na época da corrida espacial um Comando Centralizado que englobava os três ramos das Forças Armadas: exército, aérea, naval e as agências de inteligência, The US Strategic Command, o STRATCOM, sediado em Nebraska. Posteriormente, foi destinado à operação estratégica de armas nucleares e atualmente também tem como foco a guerra cibernética, nos seguintes termos:

> "USSTRATCOM is home to the critical mass of the nation's intellectual capital on strategic deterrence. In addition to our nuclear legacy, we must continue building an adaptive global warfighting command that anticipates challenges to deterring strategic attack in all domains"[20]

As dezoito agências de Inteligência nos Estados Unidos organizaram-se após os atentados aos Estados Unidos em 11 de setembro de 2001, sob o guarda-chuva da NSA, esta, por sua vez, é uma agência de inteligência mista, ou seja, civil e militar, que

[19] O artigo pode ser consultado na íntegra no sítio. Recuperado de https://www.theguardian.com/technology/blog/2009/oct/29/arpanet-internet-40 (em 08.03.2022).
[20] The US Strategic Command. Recuperado de: https://www.stratcom.mil/ (em 08/03/2022).

passou a fazer o que era até então improvável para se infiltrar na rede, dentro e fora dos Estados Unidos, e levar a cabo a espionagem eletrónica. Os Estados Unidos vêm desde então fazendo a militarização maciça do ciberespaço, do Big Data, mais recentemente da Inteligência Artificial e do *Machine Learning* para coleta e análise de dados, tanto dos inimigos quanto dos aliados, incluindo também as plataformas de entretenimento e relacionamento dos media, como Facebook, Instagram e Whatsapp. Relativamente à NSA, a agência não tem autonomia para combater em guerras e os militares americanos referem-se ao ciberespaço como algo a ser monitorado.

Os guerreiros cibernéticos estão espalhados dentro das forças armadas americanas e compõem diversos comandos com diferentes siglas, tais como *IOW (Informations Operations Wings)* que atua como centro de excelência em cibernética da Força Aérea, o *NETWARCOM (Naval Network Warefare Command)* da Marinha, e, o *AGNOSC* sob o comando e inteligência do exército. Segundo Clarke & Knake (2015), o ex diretor da NSA, Ken Minihan acreditava que "a abordagem utilizada pela NSA e pelos militares dos Estado Unidos precisa ser repensada", na opinião dele as forças armadas estão focadas na sua própria defesa e não "na contrainteligência estrangeira no ciberespaço".

O Comando Cibernético dos Estados Unidos tem o papel de defender o Departamento de Defesa dos Estados Unidos como outros órgão governamentais também, porém, não possui recursos para defender as infraestruturas civis. Essa função teoricamente deveria ser do *DHS (Department of Homeland Security)*, mas que embora seja o Departamento de Defesa Interna, Minihan afirma que o órgão não tem capacidade para defender o ciberespaço corporativo, que é o motor da economia americana e "o meio trilhão de dólares anuais de despesas do Departamento de Defesa seria inútil".

No campo da ciberespionagem, as invasões de sistemas também visam os arquivos de grandes empresas dos Estados Unidos e da Europa com o objetivo de capturar segredos industriais e militares que podem causar incalculáveis prejuízos financeiros e materiais. O número de ataques vem crescendo de tal maneira nos últimos anos que o governo norte americano criou um comité denominado National Counter-Intelligence Executive, encarregado de investigar a origem das invasões e os principais alvos. O comité apontou num de seus relatórios que os alvos principais são a industria de armamentos e as empresas de tecnologia e acusou a China e a Rússia de serem os principais responsáveis pela ciberespionagem industrial.

Os Estados Unidos têm a pretensão de dominar estrategicamente o ciberespaço e ter uma posição de vantagem em relação aos seus adversários na guerra cibernética, entretanto, a sua própria dependência do ciberespaço torna-se também a sua maior vulnerabilidade. Até hoje os Estados Unidos beneficiaram da condição geoestratégica e geopolítica, pelo fato dos maiores servidores estarem em solo americano, por serem o hub da internet e concentrarem o maior tráfego de informações, como ficou claro nas revelações feitas por Edward Snowden[21].

Snowden expôs ao mundo em 2013, o esquema norte americano de espionagem em massa que atingiu milhões de pessoas, e declarou que o "Five Eyes", uma aliança composta por cinco países: Estados Unidos, Austrália, Canadá, Nova Zelândia e Reino Unido tem não somente o objetivo de facilitação da cooperação entre as inteligências dos mesmos, mas trata-se de uma "organização de inteligência supranacional que não responde às leis de seus próprios países"[22], que partilha informações entre si de forma a contornar as "restrições constitucionais de cada país em relação a vigilância da população" e representa "a maior aliança de espionagem conhecida na história".

O Five Eyes tem origem no período pós II Guerra Mundial que visava cooperação entre as cinco nações. Posteriormente, durante a Guerra Fria foi amplamente utilizado para monitorar as comunicações da extinta União Soviética. Apesar de haver pouca informação sobre o tema, pois o mesmo é tratado com todo o sigilo que o assunto requer, sabe-se que a aliança passou por 4 fases de alargamento, nomeadamente:

- 6 Olhos: Em 2009 a França foi convidada a integrar, porém o Presidente francês, Nikolas Sarkozy, quis "garantir os mesmos status para outros aliados, incluindo a assinatura de um acordo de não espionagem", que não foi aprovado pela CIA nem pelo então Presidente dos Estados Unidos, Barack Obama.

- 9 Olhos: Composto pelos 5 juntamente com Dinamarca, França, Países Baixos e Noruega.

- 14 Olhos: Composto pelos 9 e pela Alemanha, Bélgica, Itália, Espanha e Suécia.

- 41 Olhos: Composto pelos 9 e incluindo a coligação aliada no Afeganistão.

[21] Snowden Archive: https://theintercept.com/collections/snowden-archive/ (em 08.03.2022)
[22] Chai, W.(s.d.): Five Eyes Alliance. https://www.techtarget.com/whatis/definition/Five-Eyes-Alliance (em 08.03.2022)

A estratégia dos Estados Unidos fica a dever-se em grande parte ao receio que as sucessivas Administrações revelam em relação à República Popular da China. Essa é a matéria do ponto seguinte.

2.1.2 A China

Diante dessas circunstâncias os Estados Unidos estão a tentar impedir que a China, através da Huaiwei, coloque a sua tecnologia de conexão em nuvem 5G, não somente nos Estados Unidos, mas também em vários outros países, o que permitirá que a China tenha vantagens do ponto de vista de informações, de inteligência e de tecnologias de vanguarda, e, venha a tornar-se a fornecedora dos padrões que serão seguidos por outras sociedades. Isso poderia levar ao desequilíbrio da atual Ordem Mundial, estabelecida desde o fim da segunda Guerra Mundial. De acordo com Fernandes (2019), "a ascensão a número um mundial será um restabelecimento da ordem natural das coisas, não uma subversão ou revisionismo da atual ordem internacional". E segundo Kissinger (2017, p. 419) a ordem entra em colapso quando um dos principais intervenientes deixa de desempenhar o seu papel", o que ocorrerá quando os Estados Unidos perderem a atual posição de liderança.

Outra vulnerabilidade importante a ser mencionada é a terceirização da manufatura de componentes em países como Índia e China que representa um risco pela simples possibilidade de concorrentes inserirem códigos maliciosos nos softwares que comprometeriam a segurança de todos os sistemas operacionais. Isso não significa que os Estados Unidos não reconheçam que a produção globalizada de software e hardware seja um problema. Relativamente a essa questão, e segundo Clarke & Knake (2015), no último ano do mandato o Presidente George W. Bush assinou o documento secreto denominado *Presidential Decision Dissertive* "PDD-54"[23], que, dentre vários pontos, tratava de estratégias a serem adotadas para defender o governo de passíveis ciberguerras, sendo que um dos pontos referia-se à segurança da cadeia de fornecimento.

Outro ponto crítico também refere-se à prática chinesa de subsídio de fábricas de componentes avançados fora da China financiadas pelo PCC, contratando laboratórios de pesquisas estrangeiros para desenvolver componentes que os chineses ainda não têm

[23] National Counterterrorism Center. Presidential Document: Executive Order 13354 of August 27, 2004. https://www.govinfo.gov/content/pkg/FR-2004-09-01/pdf/04-20050.pdf (em: 15.12.2022)

capacidade para produzir internamente. Essa prática é denominada de espionagem indireta e tem contribuído e muito para o avanço da indústria chinesa de microchips, pelo menos nas últimas duas décadas, ou seja, desde que integrou à OMC, em dezembro de 2001, "a China reunia as condições necessárias para assegurar o seu crescimento e a sua adesão vertiginosa como grande potência" (Rato, 2020, p. 174). Importa lembrar que a China pretende transformar-se na potência hegemónica até 2050, por isso não pode perder tempo desenvolvendo do zero algumas tecnologias.

Entretanto, para um país se transformar numa grande potência econômica e militar é preciso investir fortemente, constituindo centros de pesquisa para criação de tecnologias avançadas, cujo processo é lento, difícil e dispendioso. Paralelamente a isso, a China vem-se dedicando à atividade de espionagem e ciberespionagem para apropriação de segredos industriais e militares. O FBI tem constantemente alertado para o elevado nível de espionagem chinesa em praticamente todos os setores dos Estados Unidos, nunca antes observado, nem mesmo no tempo da Guerra Fria. Um dos métodos utilizados pelo PCC é a seleção de jovens talentos para formação de pesquisadores, professores e cientistas em áreas como física, química, eletrónica, matemática e ciência da computação que são enviados para o estrangeiro para fazerem intercâmbio técnico científico como se fossem apenas simples estudantes mas, que, na verdade, trata-se de oficiais militares doutrinados treinados para proceder de forma a não levantarem suspeitas, enviando informações sensíveis de forma segura e secreta para China. Alguns estudantes, entretanto, nem sabem que serviram como espiões, e são interrogados quando voltam para a China, obrigados a revelar o conhecimento que adquiriram, assim como através da análise e controle de todos os dados contidos nos seus computadores e telemóveis.

Além do intuito de promover ciberespionagem e a sabotagem, a tecnologia é utilizada na China também como forma ampla de controle interno total das massas em busca da perpetuação do poder, onde "a Internet pode ser usada como o mais abrangente e eficaz instrumento de controlo da vida humana alguma vez criado" (Fernandes, 2019, p. 164). Em 2017 a China organizou a Conferência Internacional da Internet, coordenada pelo Departamento de Administração do Ciberespaço chinês, na qual participaram os líderes das gigantes tecnológicas e organizações internacionais, como o Departamento de Assuntos Económicos e Sociais das Nações Unidas. Nesse evento a China, como em outras edições, reforçou seu objetivo de defesa da soberania no

ciberespaço, alinhado ao princípio da soberania dos Estados, previsto no Direito Internacional e na Carta das Nações Unidas, que concede a todos os Estados o direito de regular a Internet. Nesse caso, como no caso do Irão, trata-se da perpetuação da mesma forma de controle que exerce sobre o seu território e a sua população[24].

2.1.3 A Rússia

Halford John Mackinder foi um dos fundadores da geopolítica e da geoestratégia, num artigo em 1904 no *The Geographical Pivot of History*, no qual formulou o conceito de *Heartland*, que viria a influenciar a política externa das potências mundiais. Essa teoria previa que quem controlasse o Leste Europeu, controlaria o Heartland (Moscovo), quem controlasse o Heartland, controla a Ilha Mundo (Eurásia) e quem controla a Eurásia controlaria o mundo[25]. A profecia de Mackinder esteve perto de se concretizar ao término da 2ª. guerra mundial, período em que a União Soviética teve o maior alargamento de território para a Europa, chegando a controlar inclusive parte da Alemanha no pós guerra (Cohen, 2015).

O fim da guerra fria, entretanto foi marcado pela diminuição do território soviético, culminando com a queda da (URSS) em 1991, que conduziu à independência de 15 Estados outrora integrados na União Soviética, dentre os quais estão Estônia, Lituânia, Letônia, que hoje fazem parte da NATO, assim como muitas dessas ex-repúblicas aproximaram-se também da União Europeia, fatores que contribuíram para a atual posição de vulnerabilidade geopolítica da Rússia que está em constante busca de expansão de território, o que levou a uma estratégia russa fundamentada na guerra híbrida que vem sendo travada há décadas[26].

Mesmo após a independência em 1991, a Ucrânia manteve o controle da região da Criméia desde 1954 e, e por possuir um governo pró-russo, a Rússia controlava a base naval de Sebastopol, sede da Frota do Mar Negro, de suma importância geoestratégica. Desde a anexação da Crimeia, a região tem sido um motivo de

[24] Diário de Notícias: Governo iraniano impõe restrições ao uso de internet. https://www.dn.pt/internacional/governo-iraniano-impoe-restricoes-ao-uso-de-internet-15374517.html (em: 21.11.2022).
[25] IGES(Institute for Geopolitics, Economy and Security). Mackinder: Who rules Eastern Europe rules the World. https://iges.ba/en/geopolitics/mackinder-who-rules-eastern-europe-rules-the-world/(em: 21/11/2022)
[26] Eurodefense Portugal. A Evolução da Guerra e a 2ª invasão da Ucrânia. https://eurodefense.pt/a-evolucao-da-guerra-e-a-2a-invasao-da-ucrania/ (em: 21.11.2022).

rivalidades entre a Rússia, a Ucrânia e países europeus e os EUA. Como afirma Pagliusi "Entre nações, nunca houve amizade, mas interesses". Em resposta à anexação que foi alvo de muitas críticas internacionais, tanto os Estados Unidos quanto a União Europeia impuseram diversas sanções a indivíduos e empresas russas.

É importante evidenciar que a viragem na cena geopolítica na região deu-se em 2013 com o movimento de aproximação da Ucrânia com o Ocidente para assinar um acordo de associação com a União Europeia. Putin se opôs e fez pressão para que o então Presidente ucraniano, Viktor Yanukovich, suspendesse as negociações do acordo. Milhares de manifestantes lotaram a Praça Maidan, em Kiev, para protestar contra a política de aproximação do governo ucraniano com a Rússia, contrariamente ao interesse de aderir à União Europeia, movimento este chamado de "Euromaidan" (Oksana, Chernysh, & Susak, (2016). As manifestações foram muito violentas, através das quais a população protestava contra a corrupção e a rebelião no leste da Ucrânia apoiada pela Rússia. Yanukovich ameaçado a ponto de fugir para Rússia, ocasião em que o parlamento ucraniano elegeu um governo de transição num país dividido, liderado pelo bilionário Petro Poroshenko (Pop-Eleches & Robertson, 2018, pp. 108-117).

Paralelamente a isso, desdobrava-se uma forte campanha de informação e propaganda russa junto aos russos que naquela ocasião moravam na Ucrânia e a mobilização das tropas russas em direção ao estreito de Querche, que liga a península da Criméia com o Mar Negro. A invasão russa para anexação da Criméia em 2014, foi uma intervenção híbrida, uma estratégia militar nomeada "Maskirovika" de manipulação e dissimulação, uma guerra não somente operacional mas também de informação, utilizando narrativas russas diferentes tanto junto à Ucrânia quanto à Crimeia, com o objetivo de desinformar, tirar a atenção, confundir com o objetivo de desacreditar o governo ucraniano, culminando com um referendo controverso e fraudulento.

Desde 2014 a Rússia apoia os separatistas na região de Donbass, leste da Ucrânia, são russos, pró-russos e antigoverno, onde é travado um conflito armado entre as forças das autodeclaradas Repúblicas Populares de Donetsk e Lugansk contra o governo ucraniano, com a finalidade de alcançar a independência, apoiados financeira e militarmente pela Rússia. Em fevereiro de 2015 ambos os lados assinaram um acordo de Paz "Minsk II" seguidos de muitos outros 29 acordos de cessar-fogo firmados entre 2015 e 2020, quebrados por ambos.

Em 2019 Volodymyr Zelensky foi eleito presidente da Ucrânia através de uma vitória significativa do seu partido recém-criado, Servo do Povo, com 73% dos votos na segunda volta[27]. Ao princípio, era visto pela comunidade internacional com desconfiança, um ex-comediante que não faria frente a Vladimir Putin. Desde o inicio do seu governo, entretanto, defendeu o fim dos conflitos nas regiões separatistas e estreitou os laços com o Ocidente. Enquanto a Ucrânia se aproximava da NATO e da União Europeia, Putin reforçava sua presença militar nas fronteiras com a Ucrânia, que culminou com a invasão da Ucrânia pela Rússia em 24 de fevereiro de 2022.

Segundo Clausewitz (2014, 27) "a guerra é a continuação da política por outros meios" e esta era uma guerra híbrida que já estava a ser travada também no ciberespaço. Paglisui (2022)[28] chamou a atenção para a necessidade de perceber que a militarização do ciberespaço irrompe como "o quinto domínio da guerra – após o terrestre, marítimo, aéreo e geoespacial", onde vem sendo travados combates já há tempos, entre nações tecnologicamente mais avançadas, como a Rússia, "por meio de um novo tipo encoberto de guerra: a Guerra Fria Cibernética"[29]. O mesmo autor também afirma que esse novo tipo de combate "abrange desde ações dissimuladas de coleta de inteligência via meio digital, até a interrupção de serviços online" visando bloquear sites de sistemas financeiros, logísticos, de geolocalização e de atendimento público governamental, além da "disrupção de infraestruturas críticas do oponente, sejam civis ou militares".

Segundo (Blank 2017), a Rússia incorpora mecanismos cibernéticos e informacionais ao seu planeamento para expansão de poder. Há uma relação direta entre os ataques cibernéticos e o aspecto informacional, abordada inclusivamente num um relatório técnico da Comissão Europeia, chegando a mencionar que a "desinformação deve ser considerada uma ferramenta completamente integrada à guerra cibernética" (Flore et al. 2019).

Assim como outros Estados, a Rússia visa também controlar as portas de conexão entre o seu país e a internet global, ao aprovar a lei de proteção da seção da internet global com conteúdo russo, a Runet (Iasakova2019), assinado por Vladmir

[27] CNN (26/02/2022). Quem é Zelensky? Perfil do comediante eleito Presidente que se recusou ser fantoche e hoje é visto como herói. Recuperado de: https://cnnportugal.iol.pt/ucrania/volodymyr-zelensky/quem-e-zelensky-perfil-do-comediante-eleito-presidente-que-se-recusou-ser-fantoche-e-hoje-e-visto-como-heroi/20220228/6218e4b20cf2cc58e7e52a57. (em 02/06/2022).

[28] Paglisusi, P. (2022). Guerra Cibernética Russo-Ucraniana – Lições para o Brasil e o Mundo. Recuperado em: 24/05/2022 em: https://www.sitedaseguranca.com.br/2022/05/02/guerra-cibernetica-russo-ucraniana-licoes-para-o-brasil-e-o-mundo/

[29] Pagliusi, P., op. cit

Putin em 01 de maio de 2019, cujo objetivo é criar uma "internet soberana" e assegurar o funcionamento ininterrupto em caso de desconexão da infraestrutura global da rede. Esta lei permite ao governo russo controle total de forma a, se necessário for, cortar os serviços de Internet "de fora" em regiões inteiras do país e mesmo assim garantir que sites e serviços que utilizem a Runet tenham a conexão necessária para operar sem problemas[30]. A agência de comunicação e vigilância russa Roskomnadzor é a responsável pela coordenação tanto por garantir o funcionamento da Runet e por determinar as regras de transmissão e como será feita esta troca de Internet.

Face ao exposto, constata-se que os ataques cibernéticos constituem uma preocupação crescente para as grandes potências. Daí a sua aposta ou investimento na procura de cibersegurança. Um desiderato nem sempre atingido como se verá a seguir.

2.2 Casos Emblemáticos de Ciberataques

A lista de ciberataques de diversas naturezas que ocorreram desde 1980 é extensa, substancial e difícil de ser compilada, de acordo com Bruce Middleton (2017)[31], portanto, selecionei a seguir os mais emblemáticos. De forma a manter o foco no que se refere às implicações no contexto das tensões geopolíticas, do ponto de vista das relações internacionais, referem-se nesse capítulo apenas as ocorrências mais relevantes de ciberataques, ou seja, as que tiveram maior impacto ou causaram maiores prejuízos, não apenas na União Europeia, mas no mundo. Lembrando que não é objetivo dessa dissertação especificar detalhada e tecnicamente as abordagens utilizadas em cada ciberataque.

Um dos casos referidos por Middleton, que ocorreu em fevereiro de 2000 chama-se "*Mafiaboy"*, em que um jovem de 15 anos direcionou ataques DoS (Negação de Serviços) que afetaram sites como Yahoo!, Amazon.com, eBay, Fifa.com, CNN, dentre outros, que causaram prejuízos económicos de mais de US$ 1,7 bilhão (Osterweil, Stavrou et Zhang, 2019, pp. 1-11). Um ataque DoS como este, "consiste no envio de pacotes de solicitações para um alvo, excedendo a sua capacidade de resposta e

[30] Institute of Modern Russia (2019). Why Russia Needs a "Sovereign Runet". Recuperado de: https://imrussia.org/en/analysis/3029-why-russia-needs-a-%E2%80%9Csovereign-runet%E2%80%9D. (em 31/05/2022).

[31] Middleton, B. (2017). A History of Cyber Security Attacks 1980 to Present. CRC Press Taylor & Francis Group. Recuperado de: https://www.programmer-books.com/wp-content/uploads/2018/07/A-History-of-Cyber-Security-Attacks-1980-to-Present.pdf. Em: 17/06/2022

fazendo com que o seu servidor precise suspender o funcionamento do serviço"[32], o que faz com que o *site* saia do ar por tempo indeterminado.

O Stuxnet foi um ciberataque em 2010, batizado de "Jogos Olímpicos", desenvolvido para atacar as instalações nucleares no Irão, onde começava a ser produzido urânio enriquecido, com o objetivo de interromper o funcionamento das centrífugas, que funcionavam *offline,* para processamento do urânio. Embora o Irão tenha garantido que desenvolveria a energia nuclear para fins pacíficos, os Estados Unidos e Israel não acreditaram nessa hipótese e estabeleceram como meta incapacitar o país nesse setor. Mesmo que os Estados não tenham reivindicado esse ataque não é crível que, devido à complexidade da operação, a mesma tenha sido realizada por um grupo de hackers, sem o apoio de uma força tarefa especializada que tenha desenhado e operado softwares de infiltração e intrusão tão sofisticada, que só serviços de inteligência de alguns Estados, utilizando vastos recursos económicos e militares seriam capazes de empreender. O governo iraniano, não encontrando provas sólidas para atribuição do ataque aos governos americanos e israelita, julgou que a resposta a tais ações deveria ser feita com ataques cibernéticos contra o sistema financeiro americano e à ARAMCO saudita (Sanger 2018).

Os países em que as atividades cotidianas estão mais fortemente conectadas em rede são mais suscetíveis aos ataques cibernéticos (Maynard, 2018), como foi o caso da Estónia em 2007, primeiro país a realizar votações para cargos públicos através da Internet. Esse foi considerado o primeiro ciberataque de grandes proporções por ter afetado diretamente os sites do Governo deixando-os completamente fora do ar por mais de 22 dias. Suspeitou-se à ocasião de ter sido um ataque oriundo da Rússia, por ter ocorrido justamente na ocasião em que houve a retirada da estátua que marcava a vitória da Rússia sobre o nazismo, a estátua de bronze do Tallinn. A origem do ataque nunca foi confirmada. Entretanto, a mensagem que ficou para o mundo foi clara ao mostrar quanto os sistemas ligados à Internet são vulneráveis e deixou em alerta todos os países que têm seus serviços online e não possuem cópias de segurança, que podem ser os próximos alvos de ataques.

[32] Harán, J. (2020): "Mafiaboy" 20 anos de um dos primeiros ataques de Negação de Serviço (DoS). Recuperado de: https://www.welivesecurity.com/br/2020/02/12/mafiaboy-20-anos-de-um-dos-primeiros-ataques-de-negacao-de-servico-dos/ (em 16/06/2022).

Em 2017 o mundo conheceu o *"Wannacry"*, um ataque virtual de extensão global que atingiu não somente computadores pessoais e empresariais, mas também instituições no mundo todo, incluindo infraestruturas críticas, como o sistema de saúde público do Reino Unido. Segundo autoridades europeias, "mais de 200 mil computadores foram infectados". Embora o continente europeu tenha sido o maior alvo, conforme infográfico abaixo, divulgado pelo mesmo *site*, o país com maior número de computadores atacados foi a Rússia. Os dez países mais afetados pelo WannaCry, considerando o número de detecções foram:

1. Rússia – 113.692
2. Ucrânia – 26.658
3. Taiwan – 22.736
4. Índia – 4.108
5. Brasil – 2.114
6. Argentina – 742
7. Estados Unidos – 716
8. Japão – 648
9. Chéquia – 560
10. Grã-Bretanha – 440

Figura 2 - Os 10 países mais afetados pelo WannaCry

Fonte: https://olhardigital.com.br/especial/wannacry/ (em 21/06/2022)

De acordo com duas empresas gigantes na área de *cybersecurity*, Kaspersky e ~~a~~ Symantec, o WannaCry poderia estar vinculado à Coreia do Norte[33] e, caso fosse possível comprovar essa hipótese, essa ação cibercriminosa passaria a ser considerada um ato de ciberguerra. As Consultoras afirmaram que "boa parte do código de uma versão antiga do WannaCry, de fevereiro de 2017, também foi encontrada num malware de fevereiro de 2015 atribuído ao Lazarus Group"[34], grupo hacker que tem ligação com o governo norte-coreano. Entretanto, a utilização de parte dos códigos não é prova suficiente de que foi uma ação do mesmo grupo, que aliás, pode ter sido usado intencionalmente "to confuse anyone trying to identify the perpetrator". E ainda afirmam que o nível de sofisticação empregado por este grupo não é geralmente encontrado nas atividades de cibercrimes. "It's something that requires strict organization and control at all stages of operation. That's why we think that Lazarus is not just another advanced persistent threat actor".

A razão para o governo da Coreia do Norte estar por trás do grupo Lazarus, que é um dos principais atores de ameaças ao setor financeiro global, visa a captação de recursos para financiamento do poderio bélico do governo norte coreano. Os ataques tiveram início na Ásia e depois expandiram-se para ocidente. Segundo a ONU, as armas nucleares da Coreia do Norte foram inclusive financiadas com criptomoedas, uma vez que os programas nucleares dependem da receita dos ciberataques perpetrados pelo grupo. Estima-se que em 2019 a Coreia do Norte tenha captado cerca de US$ 2 bilhões para programas nucleares e de mísseis balísticos. De acordo com o relatório da ONU, "atores cibernéticos da DPRK [República Popular Democrática da Coreia] roubaram mais de US$ 50 milhões entre 2020 e metade de 2021 de, pelo menos, três corretoras de criptomoedas na América do Norte, Europa e Ásia"[35].

Em 2013 ocorreu um dos maiores ciberataques da história, quando 3 bilhões de contas do Yahoo foram hackeadas, ocasião em que os dados dos usuários como: nome, e-mail, números de telefone, datas de nascimento, palavras passe encriptadas foram roubadas. Essas são informações extremamente sensíveis e conveniente para quem as possuir e pretender entrar nos computadores governamentais, pois, milhões de backups

[33] Recuperado de: https://www.kaspersky.com/blog/wannacry-ransomware/16518/ (em: 21/06/2022)
[34] Recuperado de: https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group (em: 21/06/2022)
[35] Fonte: https://portaldobitcoin.uol.com.br/armas-nucleares-da-coreia-do-norte-foram-financiadas-com-criptomoedas-segundo-a-onu/ (em: 21/06/2022)

de emails pertenciam a funcionários civis de vários Governos, assim como a militares de vários países, dos quais mais de 150 mil eram americanos, onde se incluíam funcionários de agências como FBI, NSA, da Casa Branca e do Reino Unido. O Departamento de Justiça dos Estados Unidos acusou dois agentes de inteligência russa, o Serviço Federal de Segurança da Federação Russa (FSB) e dois hackers pelo ataque, devido ao papel que desempenharam na conspiração, que tinha objetivo duplo de espionagem e benefícios financeiros. De acordo com *The New York Times*[36], são eles: Dmitry Aleksandrovich Dokuchaev, cidadão e residente na Rússia e agente do FSB, Igor Anatolyevich Sushchin, cidadão e residente na Rússia, também agente do FSB, Alexsey Alexseyevich Belan, cidadão e residente na Rússia, e Karim Baratov, de 22 anos, com nacionalidade cazaquistã e canadiana e residente no Canadá. Os quatro respondem por 47 acusações criminais, que abrangem conspiração, fraude informática, espionagem económica e furto agravado de identidade.

A Procuradora Geral em exercício à época, Mary B. McCord, comentou ao supracitado periódico que "A conduta criminosa em questão, levada a cabo e de outro modo facilitada por oficiais de uma unidade do FSB que serve de ponto de contacto do FBI em Moscovo em matérias de crimes cibernéticos, é inaceitável". O ataque acarretou uma perda de 350 milhões de dólares no valor da empresa quando adquirida pela Verizon[37].

Segundo o artigo de Selena Larson[38], os dados estavam a ser vendidos na *dark web* por "piratas informáticos dispersos geograficamente, mas com base na Europa de Leste". Esta informação foi corroborada no mesmo artigo por Andrew Komarov, chefe de inteligência da InfoArmor, uma empresa de cibersegurança, que monitoriza os sítios da dark web e da deep web, regularmente usados por criminosos, espiões e afins. Segundo Andrew Komarov, houve dois compradores que eram *spammers*, com o intuito de extorsão e outro que era uma entidade que, supostamente, estava interessada em espionagem. Komarov afirma que "cada um deles pagou cerca de 300 mil dólares, mais de 286 mil euros, pela base de dados completa".

[36] Recuperado de: Fonte: https://www.nytimes.com/2017/03/15/technology/yahoo-hack-indictment.html (em 21/06/2022)

[37] Fonte: https://www.jornaldenegocios.pt/empresas/tecnologias/detalhe/yahoo-tres-mil-milhoes-de-contas-foram-pirateadas-em-2013 (Recuperado em: 21/06/2022).

[38] Larson, S. (2016): Hackers are selling Yahoo data on the dark web. Recuperado de: https://money.cnn.com/2016/12/16/technology/yahoo-for-sale-data-dark-web/, (em 21/06/2022).

Outro episódio emblemático também foram os ataques cibernéticos à Sony em 2014, atribuídos à Coreia do Norte. A empresa faria naquele ano do lançamento do filme "A Entrevista", uma paródia do regime comunista sobre um complô para assassinar o líder da Coreia do Norte, Kim Jong-un, quando a sua rede interna de computadores foi hackeada. O grupo responsável pelo ataque autodenominado *The Guardians of Peace* (GOP) "ameaçou vazar dados secretos da multinacional japonesa ao mundo caso suas demandas não fossem atendidas"[39].

Os hackers disponibilizaram filmes da Sony que ainda que ainda não haviam estreado em *sites* piratas, sendo que "A Entrevista" não estava entre esses filmes. Além disso, divulgaram os salários e os números de segurança social de milhares de empregados da Sony – incluindo de celebridades. O grupo fez também ameaças de ataques terroristas nos cinemas em que o filme fosse exibido, o que levou à recusa por parte de redes americanas de cinema de exibição do filme. A Sony acabou por cancelar o lançamento do filme.

Wakefield menciona no seu artigo que, de acordo com serviços de inteligência americanos, o GOP está ligado à capital norte-coreana, Pyongyang. As suspeitas também recaem sobre a nomeada Unidade 121, a divisão de elite de hackers do governo norte-coreano, que faz parte do Escritório Geral de Reconhecimento (RGB, em inglês), responsável por operações clandestinas. Contudo, o governo norte coreano sempre negou o seu envolvimento e inclusive ofereceu ajuda aos Estados Unidos para descobrir os verdadeiros responsáveis, alegando que outros governos simpatizantes da sua causa poderiam ser os responsáveis.

Os especialistas divergem quanto aos possíveis responsáveis. No mesmo artigo, Marc Rogers diz que o código do ataque remete a um computador com IP da Coreia, porém, a linguagem torna menos provável que a fonte tenha sido a Coreia do Norte e levanta a hipótese de hackers chineses estarem por trás do ataque.

Já na opinião de Sean Sullivan, executivo da empresa de segurança F-Secure, a extorsão pode ter sido o motivo do ataque, porque "uma motivação financeira é muito mais crível do que um ataque coordenado por um país". Além disso, afirma ser "muito mais provável que a Coreia do Norte tenha recrutado hackers chineses que buscam ganhar dinheiro fácil e, ao mesmo tempo, desestabilizar a Sony".

[39] Wakefield, J. (2014): Entenda o ataque virtual à Sony. Recuperado de: https://www.bbc.com/portuguese/noticias/2014/12/141220_entenda_coreia_norte_lgb (em: 22/06/2022)

Faltam até hoje provas para relacionar o governo norte-coreano diretamente ao ataque e com isso, muitas outras especulações e teorias da conspiração continuam a pairar no ar.

Também os Estados Unidos não escapam aos ciberataques. Assim, por exemplo, em 2016, o ataque cibernético ao Partido Democrata dos EUA teve grande repercussão mediática acerca da responsabilidade de uma agência de internet russa e uma dúzia de hackers quanto à interferência na campanha eleitoral americana em prol da eleição de Donald Trump, por meio de operações de ciberespionagem para obter informações privilegiadas (Cole et al, 2017). Levou dois anos para que o Departamento de Justiça americano apresentasse denúncia formal contra agentes de inteligência russos envolvidos no ataque. De acordo com a denúncia, "os 12 russos trabalhavam para o GRU, o departamento central de inteligência do Kremlin" com o objetivo de interferir nas eleições americanas[40], tendo inclusive tentado corromper o sistema de votação americano, sem sucesso. No ataque foram roubados os dados de 500 mil eleitores americanos, além de dados sensíveis de políticos do Partido Democrata. A lista abrangia também vários congressistas que fazem parte dos Comités de Inteligência, de Serviços Armados e de Relações Exteriores, cuja utilização indevida de dados poderia ter inclusive sérias consequências para a segurança nacional americana de acordo com relatório do Departamento de Justiça, publicado em março de 2019[41].

Carazzai menciona que a denúncia acusou os russos de 11 crimes, entre eles, "crime contra os EUA por meio de operações cibernéticas, roubo de identidade e lavagem de dinheiro", o Partido Democrata defendeu que esse foi "um ataque contra eleitores americanos" e o Presidente do Comité Nacional Democrata afirmou que "os esforços do Kremlin para perturbar o processo eleitoral têm graves implicações na democracia." Donald Trump sempre negou envolvimento com os russos em favorecimento da sua campanha e desvalorizou a investigação liderada pelo FBI denominando-a de "caça às bruxas".

De acordo com a agência Reuters, o gabinete de Robert Mueller, então Diretor do FBI que investigou a Casa Branca, afirmou numa conferência de imprensa em junho de

[40] Carazzai, E. (2018): EUA denunciam russos por ataque hacker a democratas. Recuperado de: https://br.noticias.yahoo.com/eua-denunciam-russos-por-ataque-003100504.html (Em: 22/06/2022)
[41] U.S. Department of Justice. (2019): Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Recuperado de: https://www.justice.gov/archives/sco/file/1373816/download. (em 22/06/2022).

2017 que a conspiração teve início em 2014[42]. Segundo a agência, Rod Rosenstein, vice-secretário de Justiça dos EUA, fez as acusações e disse também que a investigação não havia sido ainda finalizada. Rosenstein afirmou em conferência de imprensa que "a acusação alega que conspiradores russos queriam promover discórdia nos Estados Unidos e prejudicar a confiança pública na democracia. Nós não podemos deixá-los ter sucesso".

Influenciar resultados de processos democráticos alheios não é uma prática incomum, uma vez que a vitória de determinados partidos afeta diretamente não somente a política interna, mas também a externa dos países. De forma a obter vantagens e atender seus interesses políticos, económicos ou até mesmo ideológicos, Estados fortes vêm exercendo consistentemente ao longo da História, influência em processos eleitorais, como é o caso dos Estados Unidos e da extinta União Soviética, através de ajuda financeira a partidos políticos ou através de pressões ou ameaças de cortes de fundos de ajuda internacional por exemplo.

Apesar das interferências externas em eleições não constituírem algo novo, a interferência russa nas eleições norte-americanas "representa uma tendência na qual o meio cibernético torna-se um valioso novo recurso"[43], o que é extremamente preocupante visto que os processos democráticos em si estão a ficar cada vez mais vulneráveis com o avanço e uso indevido da tecnologia da informação e do ciberespaço que representam novas formas de intervenção nos processos eleitorais. Para além do caso americano, há outros exemplos em outros países, que tiveram menor repercussão e cobertura mediática, como é o caso da Alemanha e da França.

Segundo Schwirtz (2017) há suspeitas que a Rússia tenha utilizado de estratégia semelhante para interferir na campanha eleitoral alemã de 2017 com o objetivo de prejudicar a reeleição da chanceler Angela Merkel, pelas críticas que fazia, à época, à política da Rússia, nomeadamente em relação à Ucrânia.

De acordo com Breeden, Aurelien; Chan, Sewell; Perloth Nicole (2017), grupos ligados à Rússia, possivelmente envolvidos com os ciberataques relacionados com o processo eleitoral americanos de 2016, vazaram dias antes da votação uma data de

[42] Strobel, W. & Volz, D. (2017): Russos são indiciados por interferência na eleição dos EUA de 2016 para impulsionar Trump. Recuperado de: https://www.reuters.com/article/eua-russia-indiciamento-idBRKCN1G02GR-OBRTP. (em 22/06/2022)

[43] Honório, T. O uso de ciberataques em eleições e as Relações Internacionais. Mural Internacional: V. 9/N. 1, 2018. Recuperado de: https://www.e-publicacoes.uerj.br/index.php/muralinternacional/article/view/32570 (em 07/07/2022).

documentos concernentes à campanha do então candidato Emmnuel Macron com o objetivo de impedir que o candidato tivesse tempo útil de manobra para aliviar o impacto negativo que os documentos gerariam para sua campanha.

O governo de Malta também acusou a Rússia de ciberataques e interferência em seu processo eleitoral em 2017 (Doward, 2017), quando assumiu a presidência do Conselho de Ministros da Europa, tendo passando a desempenhar uma posição estratégica para o estabelecimento da agenda política da Europa. Os ciberataques têm sido parte da estratégia atual russa de ciberguerra, utilizada de forma recorrente para interferência em diversos processos eleitorais do mundo.

Em 2017, uma das três maiores empresas americanas de crédito, a Equifax, foi alvo de um ataque hacker que roubou dados de 143 milhões de pessoas. De entre os dados constávam nomes completos, endereços de e-mail, carta de condução, morada, números de segurança social, datas de nascimento, números de cartões de crédito e outras informações igualmente sensíveis. O acesso irregular ocorreu entre maio e julho, mas foi divulgado apenas em agosto, quando a companhia levou o caso às autoridades e contratou uma empresa de cibersegurança independente para conhecer a abrangência do ataque e investigar em detalhes a ação dos hackers. O caso levantou mais uma vez a necessidade de as empresas implementarem políticas de proteção de dados como parte do compromisso com o cliente e levou à queda brusca das ações da empresa e à renúncia do então CEO da empresa, Richard Smith[44].

Nesse caso, as informações pessoais vazadas seriam usadas para aplicar os mais diversos golpes individualizados, em forma de *phishing*, por exemplo. O *phishing* normalmente é realizado através de e-mail, redes sociais, SMS ou outros meios e segue um mesmo padrão. O golpista elabora uma mensagem personalizada, com o objetivo de induzir a vítima a clicar num link, baixar um anexo, enviar as informações solicitadas, como senhas pessoais ou até mesmo efetuar um pagamento real. Desta forma, "a maioria dos casos phishing pode levar ao roubo de identidade ou dinheiro e também é uma técnica eficaz para espionagem corporativa ou roubo de dados"[45]. Sem mencionar que para além de tudo isso, um banco de dados dessa dimensão tem um alto valor agregado na *Deep Web*.

[44] Reuters (2017): Equifax diz que vulnerabilidade em servidor levou a ataque de hackers. Recuperado de: https://www.reuters.com/article/tech-equifax-vazamento-idBRKCN1BP1XL-OBRIN (Em: 11/07/2022).
[45] Avast (s.d.): O guia essencial sobre phishing. Recuperado de: https://www.avast.com/pt-br/c-phishing. (em 11/07/2022).

As investigações do FBI iniciaram-se em 2017, até que em 2020 foi possível rastrear os 40 endereços de IP envolvidos no ataque. Com isso, as autoridades conseguiram chegar até aos quatro membros envolvidos. Numa conferência de imprensa em fevereiro de 2020, o Departamento de Justiça dos Estados Unidos acusou formalmente quatro hackers militares chineses: Wu Zhiyong, Wang Qian, Xu Ke e Liu Lei, que também foram indiciados pela provável ligação com "roubos de segredos comerciais, propriedade intelectual e informações confidenciais de empresas americanas nos últimos anos"[46]. Durante a conferência, o procurador-geral dos Estados Unidos, William Barr, e o vice-presidente do FBI, David Bowdich, "classificaram o episódio como o maior caso de invasão patrocinada pelo estado já descoberto".

Em 2022 veio à tona o ciberataque realizado em dezembro do ano anterior à empresa Sky Mavis, responsável pelo desenvolvimento do videojogo *Axie Infinity*, que perdeu o equivalente a mais de 540 milhões de euros[47], sendo, até ao momento, considerado o maior roubo de criptomoedas da história.

A empresa vietnamita que desenvolveu o jogo, diz que os *hackers* se aproveitaram de uma falha oculta no sistema e obtiveram as senhas de acesso às contas para realização das transações digitais com criptomoedas. A Sky Mavis está a trabalhar com uma empresa americana que investiga fraudes e sistemas de lavagem de dinheiro, para tentar recuperar os fundos e identificar a identidade dos hackers, que inicialmente levou a Sky Mavis a cinco endereços suspeitos. Assim, "a assinatura deixada na validação dos nós chamou a atenção do grupo que trabalha no caso, que inclui criptólogos forenses e autoridades reguladoras"[48].

As investigações, como de praxe, correm sob sigilo, mas em 14 abril de 2022, agentes do FBI já puderam apontar hackers da Coreia do Norte como possíveis

[46] Nogueira, L. (2020). EUA acusam quatro hackers chineses de roubar dados de americanos. Recuperado de: https://olhardigital.com.br/2020/02/10/seguranca/eua-acusam-quatro-hackers-chineses-de-roubar-dados-de-americanos/. (em 11/07/2022).

[47] Público.pt (2022): "Hackers" roubam mais de 540 milhões de euros em jogo "online". Recuperado de: https://www.publico.pt/2022/03/31/tecnologia/noticia/hackers-roubam-540-milhoes-euros-jogo-online-2000887. (em 11/07/2022).

[48] Sousa, R. (2022): Maior roubo em criptomoedas da história: plataforma do Axie Infinity (AXS) sofre ataque hacker e criminosos levam US$ 625 milhões. Recuperado de: https://www.seudinheiro.com/2022/criptomoedas/axie-infinity-axs-ataque-hacker-criptomoedas/. (em 11/01/2022).

culpados. De acordo com as autoridades, "o Grupo Lazarus, conhecido por ser comandado por norte-coreanos, seria o responsável pelos ataques"[49].

Segundo Santana, V. (2020, p. 5), as organizações criminosas transnacionais utilizam criptomoedas para compras ilegais de armamentos, lavagem de dinheiro e outras atividades ilícitas ciberterroristas para fortalecer suas estruturas, sua forma de agir e cometer delitos de maior gravidade, como tráfico de armas, pessoas, drogas e financiamento do terrorismo, passando a ser um problema sem fronteiras, para a Defesa Nacional de todos os países e que podem inclusive causar efeitos devastadores na sociedade (Hansen & Nissenbaum (2009, p. 1155).

Não poderia deixar de destacar também o panorama atual das principais modalidades de ameaças no ambiente cibernético na União Europeia, na tabela (Anexo, Tabela I, p.I), elaborada pela ENISA – Agência de Cibersegurança da União Europeia, onde constam os tipos de ameaça com uma breve descrição das mesmas, relativamente ao ano de 2021[50]. A ENISA emite relatórios anuais com a panorâmica dos resultados da investigação documental referente ao ano anterior e divulgou em seu relatório de 2021 um aumento significativo em relação a 2020 no volume de incidentes de cibersegurança e dos indicadores de cibercrime na União Europeia. Para cada uma das ameaças identificadas, o relatório aborda as técnicas de ataque, os incidentes e as tendências relevantes, além das medidas de mitigação propostas. "Simultaneamente, identifica os cibercriminosos e os agentes estatais como os principais agentes de ameaças no ciberespaço de interesse nacional"[51].

Para efeitos de comparação em relação ao relatório realizado em 2020, o infográfico da ENISA (Anexo, Tabela II, p.II) demonstra o ranking das 15 principais ameaças e as respectivas "trends", ou seja, tendências em ascenção (↑), em declínio (↓) ou em estagnação (→)[52].

[49] Pinto, B. (2022): Maior roubo em cripto da história. Recuperado de: https://www.seudinheiro.com/2022/criptomoedas/roubo-de-criptomoedas-axie-infinity-bdap/. (em 11/07/2022).

[50] Fonte: Adaptado de Conselho da União Europeia - Principais ciberameaças na EU.(dados de abril de 2020 a julho de 2021). https://www.consilium.europa.eu/pt/infographics/cyber-threats-eu/ (em: 16.06.2022)

[51] Fonte: ENISA (2021). Recuperado de: https:// www.enisa.europa. eu/publications/ enisa-threatlandscape-2021 (em 16.06.2022).

[52] Fonte:https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats (em 21.08.2022).

A agência considera no seu essencial que:

> "Os ciberataques não conhecem fronteiras. Todos os estratos sociais podem ser afetados e a União deve estar pronta para responder a ciberataques (em grande escala e transfronteiriços) e a cibercrises em massa." (https://www.enisa.europa.eu/about-enisa/about/pt)

Figura 3 - Diagrama sobre o cenário das ameaças segundo a ENISA

Fonte: https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_pt.pdf. Recuperado em 16.06.2022

Relativamente ao prognóstico das ameaças cibernéticas e o que os líderes podem fazer para proteger suas organizações, assim como às tendências de segurança cibernética que impactarão as economias e as sociedades nos próximos anos, o Cybersecurity Outlook 2023, de janeiro de 2023, traz as pesquisas mais recentes sobre o tema[53].

Carrapiço e Barrinha (2016, p. 256) consideram que a natureza do ciberespaço é crítica no que se refere à questão do privado e do público, também quanto à responsabilização nacional ou internacional e por consequência tornou-se uma prioridade nas Relações Internacionais. Para Nunes (2012, P.116) salvaguardar o ciberespaço (cibersegurança) é uma obrigação nacional, primordial para assegurar a "soberania e a sobrevivência do país".

[53] Insight Report (2023). Global Cybersecirity Outlook 2023. https://www.weforum.org/reports/global-cybersecurity-outlook-2023/ (em: 08.05.202)

Importa clarificar que a cibersegurança distingue-se da ciberdefesa, pois ambas contemplam ações específicas no ciberespaço (Militão, 2014, p.25). A cibersegurança está relacionada às forças policiais e serviços informáticos enquanto que a cibersegurança é proveniente das forças armadas e também abrange as atividades relacionadas ao cibercrime, hackitismo, ciberespionagem e ciberterrorismo.

Para Cavelty (2010), a cibersegurança se divide em três tipos de ameaças: cibercrime, ciberterrorismo e ciberguerra. Esta última "refere-se às ações levadas a cabo por um Estado nação para aceder ao computador de outra nação com o intuito de danificar ou causar disrupção". Barrinha e Carrapiço (2016, p. 252) citam Arquilla e Ronfeldft (1993) a se referirem que a ciberguerra é "uma guerra focada no conhecimento sobre quem sabe o quê, quando, onde, porquê e sobre o grau de certeza que uma sociedade ao exército que tem relativamente à informação que dispõe sobre si mesmos e sobre o adversário. Importa dizer que mesmo antes da ofensiva militar da Rússia contra a Ucrânia em 25 de fevereiro de 2022, ambos Estados-nações já travavam há anos uma ciberguerra encoberta, como será abordado a seguir.

Capítulo III

3. A Nova Guerra Fria

3.1 A Guerra no domínio cibernético Russo-Ucraniana

Um confronto velado entre a Rússia e a Ucrânia vem sendo travado desde o fim da extinta União Soviética em 1991. Apesar dos primeiros ataques a sistemas de informação de empresas privadas e instituições estatais da Ucrânia terem sido registrados durante os protestos em massa em 2013, a arma cibernética russa denominada 'Uroburos', um pacote de *Malware* produzido por uma agência do governo russo[54], existe desde 2005. Os ataques cibernéticos entre a Rússia e a Ucrânia vêm se intensificando há uma década e são precursores da guerra cinética que teve início em 2022. Em entrevista a Suzuki (2022, 1 de março) Luca Belli, afirma que "desde a anexação da Crimeia em 2014 os russos vêm desenvolvendo competências de ponta no âmbito de ciberataque e ciberdefesa" e afirma também que "ao longo desse tempo eles vêm testando, experimentando e até implementando essas tecnologias em uma escala ampla". Belli afirma também que "essa é uma guerra híbrida, uma guerra que combina as táticas bélicas clássicas - invasão com tropas e tanques - às estratégias cibernéticas".

A estratégia de guerra cibernética envolve não somente ações ofensivas "que visam destruir, impedir, dificultar o uso de informações cibernéticas do inimigo por ataques físicos cibernéticos, via rede, com armas cibernéticas", como ações defensivas "que visam evitar ou minimizar ataques cibernéticos lançados pelo inimigo, protegendo informação, e restaurar rapidamente danos e limitações que o oponente venha a provocar", mas também ações de exploração "que visam monitorar o inimigo em busca de informações sigilosas, detectar atividades cibernéticas e conhecer as suas vulnerabilidades sistêmicas na rede, buscando informações que possam trazer vantagem para quem as realiza" (Pagliusi, 2022).

Neste capítulo estão listados os ciberataques gerados por ambos os lados. Nota-se, pelo êxito das operações e ataques em massa, a predominância da Rússia em relação à Ucrânia, "em face ao melhor preparo tático das tropas russas no quinto domínio da

[54] The Epic Turla (snake/Uroburos) attacks. https://www.kaspersky.com/resource-center/threats/epic-turla-snake-malware-attacks. (em 12.10.2022)

guerra" (Pagliusi, 2022). Opinião compartilhada por (Giles, 2012a, pp. 1-3) ao afirmar que "a Rússia lidera mundialmente o desenvolvimento de software e técnicas na área de cibersegurança". De acordo com o pensamento de Weedon (2015), os russos consideram as operações na rede de computadores como um instrumento integrado aos esforços do Estado para manter e/ou ampliar o domínio político e militar em um determinado território.

A ação militar russa na Ucrânia em 2014/2015, também foi acompanhada por uma série de ataques de natureza DDoS, "semelhantes aos que paralisaram os sistemas de computadores na Estônia, em 2007, e atingiram as comunicações e o Banco Nacional na Geórgia, em 2008, marcando o início de uma nova era do ciberconflito" (Kello, 2013, p. 24). Uma data de ataques da mesma natureza também infectaram computadores de estações elétricas e derrubaram o fornecimento de energia na Ucrânia (Geers, 2015).

Diante destes fatos, a guerra Rússia-Ucrânia vem sendo profusamente titulada como a crise de segurança mais grave desde o fim da Guerra Fria. Na verdade, "o conflito em questão, atualmente, é o maior exemplo do que se convencionou denominar como guerra híbrida, uma espécie de conflito que combina estratégias militares, econômicas e políticas para atingir os objetivos de um determinado Estado em território inimigo" (Limnell, 2015, p.521). Stowell (2018) refere-se ao termo guerra híbrida ou ameaça híbrida como o "uso da força militar convencional, apoiada por táticas de guerra irregular e *cyber"*. Para Visacro (2018, p. 157) "a vitória tornou-se incerta, uma vez que deixou de ser prerrogativa dos soldados alcançá-la no campo de batalha".

A NATO (2016, p.14) reforça esta ideia referindo que para combater uma ameaça de natureza híbrida é preciso que seja realizada uma "articulação de respostas de natureza idêntica", isto significa, "a combinação de respostas militares e não-militares, através do emprego coordenado de todos os instrumentos do Poder". Na prática, o combate às ameaças híbridas requer a conjugação de medidas passivas e ativas de forma a aumentar a capacidade de resiliência de um Estado para evitar ou reduzir o impacto dos mesmos e, paralelamente, "estabelecer um quadro de medidas a serem implementados para preparar, proteger e recuperar as funções e estruturas mais suscetíveis de serem alvos de ataques" (Hagelstam & Narinen, 2018).

3.1.1 Os ciberataques russos contra a Ucrânia de 2013 a 2022

Em 2013 foi iniciada a "*Operação Armageddon"*, campanha russa de ciberespionagem sistemática nos sistemas de agências governamentais, policiais e de defesa ucranianos, com o objetivo de apoiar a Rússia no campo de batalha. Este suporte ao instrumento militar deu o seu primeiro indício de atividade a 20 de fevereiro de 2014, período em que ocorreram violentos confrontos em Kiev, e paralelamente as unidades militares russas e ucranianas na Crimeia estavam preparadas para entrar em ação (Kofman, et al., 2017). O caos instalou-se quando o Presidente Yanukovich abandonou a Ucrânia e a Rússia destacou elementos do 45º Regimento Independente VDV SPETSNAZ para fomentar a revolta da população, facilitada pelo vazio de poder e a forte oposição ao novo governo de Kiev existente na Crimeia, principalmente em Sebastopol, onde Yanukovich foi eleito com a maioria de 84% das intenções de votos (Ramos, 2019).

Através da prática conhecida como *'troll*' na internet, o governo russo financiou pessoas que fizessem comentários pró-Rússia em redes sociais, blogs, vídeos e sites de notícias, com o "objetivo de disseminar uma campanha de desinformação, legitimar a anexação da Crimeia e apoiar os separatistas no leste ucraniano" (Barboza, 2018, pp. 54-55). De acordo com Benedictus (2016), " a maior parte do que sabemos vem de uma série de vazamentos em 2013 e 2014, a maioria deles diz respeito a uma empresa de São Petersburgo chamada Internet Research Agency, depois renomeada como Internet Research". O mesmo autor afirma que é provável que "seja uma das várias firmas onde os trolls são treinados e pagos para denegrir adversários de Putin, tanto no país como internacionalmente". Mais acrescenta que "de acordo com documentos divulgados por um grupo de hackers em 2013, a Internet Research Agency empregou mais de seiscentas pessoas em toda a Rússia e teve um orçamento anual de US$ 10 milhões – metade pago em dinheiro". Ainda segundo a mesma fonte, "os funcionários tinham como tarefa postar comentários em artigos de notícias cinquenta vezes por dia", sendo que "aqueles que escreviam blogs tinham que manter seis contas no Facebook e publicar pelo menos três cinquenta e cinco posts diários". Além disso, "no Twitter, eles precisavam ter pelo menos dez contas, nas quais postavam cinquenta

vezes. Todos tinham metas para o número de seguidores e o nível de engajamento que precisavam atingir".

A análise da citação não permite dúvidas sobre a importância que o Kremlin dá a esta forma de obter informações e promover desinformação.

Um componente fundamental para a construção da narrativa russa é a divulgação de propaganda, informação e campanhas de desinformação em larga escala que, somadas ao crescente uso de ataques cibernéticos, compõem parte da sua estratégia de Guerra da Informação. São vários os meios em que são empregadas técnicas para disseminar e ou, obter, distorcer, desacreditar, falsificar informações de inteligência, como está relacionado no quadro a seguir. O vazamento dessas informações para a Comunicação Social ocorre nomeadamente, no momento mais oportuno.

Figura 4 - Meios de persuasão utilizados para a construção da narrativa russa

Operações de Informação - Meios de influência	
	**Russia Today** - lançada em 2005, tinha orçamento de US$ 350 milhões em 2015. Concentra-se em desacreditar a imagem e as políticas do Ocidente, bem como qualquer percepção de uma verdade objetiva.
	**Sputnik** - lançada em 2014, com orçamento de US$ 140 milhões. Plataforma online que opera paralelamente à RT. É uma modernização da clássica infraestrutura e das ferramentas de informação soviéticas. A Sputnik é um modelo de *infotainment*, com conteúdo multimídia atrativo, focando em notícias locais e usando a credibilidade de jornalistas conhecidos. Está em expansão. Tem abrangência inclusive no Brasil.
	**Russia Beyond the Headlines** (RBTH) e **Russia Direct** (RD) - A RBTH busca parcerias com jornais ocidentais de reputação para parecer isenta e objetiva, enquanto mantém fortes laços com organizações patrocinadas pelo governo russo. A RD produz *newsletters* e reportagens especiais, parecendo uma fonte de informação legítima sobre a Rússia, enquanto é, extraoficialmente, parte da rede do Kremlin.
	**Mídias sociais** - Moscou emprega *trolls* que postam propaganda pró-Rússia, sob falsas identidades. As operações nas mídias sociais são destinadas a frustrar *websites*, retardar trabalhos jornalísticos e reduzir a utilidade da internet como um espaço democrático.
	**Grupos de compatriotas russos** - Esses grupos representam infraestrutura crítica para os esforços de influência de Moscou, servindo como ligação para influenciar países com populações de língua russa. Trata esses compatriotas como ferramentas para políticas em países vizinhos, para construir a imagem da diplomacia russa ou legitimar a política externa que interfere nos assuntos de outros países.

Fonte: adaptado de Zakem & Warner (2017). Recuperado de: https://bdex.eb.mil.br/jspui/handle/123456789/3868 (em 16/10/2022).

Relativamente a este ponto importa realçar que as designações sofrem alterações, sobretudo quando a Rússia pretende contornar algumas das críticas que lhe são feitas, assim por exemplo o site "*Russia Beyond The Headlines"* passou a designar-se apenas como "*Russia Beyond"*[55].

Rutenberg (2017) menciona o relatório das agências de inteligência do governo dos EUA que destaca a influência desses meios de comunicação financiados pelo governo Putin, o canal "*Russia Today"* e o resto da máquina de informação russa estavam sendo empregues pelo setor de inteligência russo para sabotar a ordem democrática nos Estados Unidos da América e manipular as eleições norte-americanas em 2017.

A Operação "*Snake"*, implementada em 2014 pela Rússia, tratava-se de uma campanha que utilizava ferramentas de espionagem cibernética muito maior do que se sabia anteriormente. Segundo relatório da BAE System, uma empresa de segurança alemã, os autores e operadores do Snake eram profissionais comprometidos e bem financiados, tendo em conta "a complexidade do malware e a gama de variantes e técnicas usadas para apoiar seu funcionamento e desenvolvimento"[56]. Grupos pró-Rússia, como o '*CyberBerkut*', assumiram a autoria do ataque *hacker* ao sistema central da comissão eleitoral com o objetivo de adulterar o resultado da eleição presidencial. O grupo teve acesso a telemóveis de parlamentares ucranianos que foram invadidos ou bloqueados. Foi registrado um incremento no volume de ataques cibernéticos russos em sistemas de TI, tendo como principais vítimas "agências governamentais, da União Europeia, dos EUA, agências de defesa, organizações internacionais e regionais de defesa e políticas, '*think tanks'*, organizações de mídia e de dissidentes ucranianos" (Pagliusi, 2022). Weedon (2015) afirma que apesar do ataque ter causado alguns danos, o serviço de inteligência ucraniano foi capaz de eliminar o *malware* que havia infectado o sistema eleitoral e alterar o software sem repercussões negativas no processo das eleições.

Em dezembro de 2015, o ataque denominado *'BlackEnergy'*, atingiu os sistemas operacionais de uma fábrica elétrica em Ivano-Frankivsk, situada no oeste da Ucrânia, comprometendo a distribuição de energia e o abastecimento de milhares de

[55] Russia Beyond the Headline: https://www.rbth.com/ (em 18.10.22).

[56] Fonte: BAE Systems. Recuperado de: https://web-archive-org.translate.goog/web/20200722022109/https://www.baesystems.com/en/cybersecurity/feature/the-snake-campaign?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=wapp (em 18/10/2022).

residências e deixou a cidade sem luz por mais de seis horas. O ministro ucraniano de Energia acusou a Rússia de estar por detrás dos ataques (Tuptuk & Hailes, 2016). Em 2016 houve um segundo ataque à rede elétrica da Ucrânia, hackers russos cortaram a eletricidade na capital Kiev, uma ofensiva sem precedentes.

No ano seguinte, em 2017, Moscovo ordenou o ataque cibernético conhecido como *NotPetya*, que visava inicialmente afetar empresas privadas ucranianas, mas que acabou por se disseminar em todo o mundo. "O *NotPetya* se disfarçou de *ransomware*, mas na realidade era um código puramente destrutivo e altamente viral" [57].

Segundo Kramer (2022) em janeiro de 2022 foram realizados ataques a sites do governo ucraniano, um dia após o fracasso das negociações entre EUA-Rússia sobre o futuro da Ucrânia na NATO. Após as negociações entre o Ocidente e Moscovo com o objetivo de impedir uma invasão russa atingirem um impasse, o site do Ministério das Relações Exteriores ucraniano foi desfigurado mostrando a mensagem: Tenha medo e espere o pior. Por ser complexa a comprovação da origem do ataque, o Ministério ucraniano decidiu não acusar diretamente a Rússia, apesar do longo histórico de ataques cibernéticos russos contra a Ucrânia.

A partir de fevereiro de 2022, depois que tropas russas invadiram a Ucrânia, ocorreram inúmeros ataques em massa contra sites governamentais e bancários ucranianos. A inteligência americana atribui tais ações a ciberatacantes russos, embora o governo russo continue a negar qualquer envolvimento nessas ações e afirmar que nunca conduziu e não conduzirá nenhuma operação maliciosa no ciberespaço (Pagliusi, 2022).

A Tabela III do Anexo (p.III) apresenta a síntese dos principais ciberataques russos contra a Ucrânia, mencionados nesse capítulo, no período de 2013 até fevereiro de 2022. Importa por isso dizer que a guerra fria cibernética entre ambos os países veio a ser construída ao longo de uma década. Esta guerra, no entanto, não terminou quando o presidente russo Vladmir Putin autorizou em 24 de fevereiro de 2022 a 'Operação Militar Especial" para invadir efetivamente o território ucraniano. De facto, a entrada em ação dos instrumentos de guerra tradicional não inviabiliza, bem pelo contrário, a continuação do recurso ao elemento cibernético.

[57] https://mittechreview.com.br/como-uma-guerra-cibernetica-russa-na-ucrania-pode-se-espalhar-globalmente (Recuperado em em: 18/12/2022).

3.1.2 Os ciberataques ucranianos contra a Rússia de 2016 a 2022

Em 2014 os hacktivistas ucranianos que atuavam de forma independente passaram a direcionar os seus conhecimentos para a proteção do ciberespaço ucraniano e, posteriormente, uniram-se para realizar operações conjuntas, em consonância com o Art. 17 da Constituição Ucraniana, que garante a todo o cidadão ucraniano o direito e o dever de defender a independência de seu país e sua integridade territorial.

A Aliança Cibernética Ucraniana (UCA, *Український кіберальянс* , УКА)[58] foi criada na primavera de 2016 e é formada por uma comunidade de ciberativistas ucranianos não somente residentes na Ucrânia, mas também no mundo. Integram a UCA os dois ciberativistas '*FalconsFlame' e 'Trinity'*, que posteriormente se uniram ao grupo "RUH8 e ciberativistas individuais do grupo CyberHunta". De acordo com o '*Inform Napalm'*[59], site criado em 2014, a "Aliança Cibernética Ucraniana transmite exclusivamente os dados extraídos para análise, reconhecimento e publicação à comunidade de inteligência internacional, bem como às agências policiais da Ucrânia", a partir de "uma iniciativa voluntária para informar os cidadãos ucranianos e o público estrangeiro sobre a guerra russo-ucraniana e as atividades dos serviços especiais russos" (InformNapalm, 04/11/2022). Em 2016 a UCA, liderada por '*FalconsFlame' e 'Trinity'* hackeou o servidor corporativo do canal russo '*Channel One'*. O ataque tinha como objetivo principal forçar a Rússia a desocupar a região de Donbass e cumprir suas obrigações relativas aos acordos de Minsk[60].

Segundo o Warsau Institute (2017, 10 de outubro), em 2016 a operação DonbasLeaks a UCA realizou mais de cem ataques *hackers* a "sites e caixas de correio de militantes, propagandistas, seus curadores e organizações terroristas que operam nos territórios ocupados". Sendo um dos alvos a caixa de correio eletrónico da organização russa chamada 'União de Voluntários do Donbass'.

Em outubro de 2016 a Operção SurkovLeaks constituiu no vazamento de 2.337 e-mails com centenas de anexos sigilosos, datados entre 2013 e 2014, que denunciavam haver planos concretos para se tomar a Crimeia da Ucrânia e promover distúrbios separatistas em Donbas. Os vazamentos estão relacionados ao período em que a Rússia tentava colocar em prática seu projeto 'Novorossiya' (Nova Rússia), de 2014 em diante,

[58] Ukranian Cyber Alliance. https://cyber.org.ua/ (em: 19.10.2022).
[59] Inform Napalm. https://informnapalm.org/en/tag/ukraine/ (em: 19.10.2022)
[60] Acordos de Minsk. https://www.europarl.europa.eu/ftu/pdf/pt/FTU_5.6.3.pdf (10.09.2022)

com o objetivo de separar o sudeste da Ucrânia. "Quando isso falhou, exceto pelos estados que haviam sido estabelecidos em Donetsk e Luhansk, o Kremlin passou a promover um movimento separatista na Ucrânia, cujo objetivo final era sua federalização. Esta campanha continua hoje" (Shandra, A. & Seely, R., 2019).

Em 25 de fevereiro de 2022, Mykhailo Fedorov, Vice-Primeiro-Ministro e Ministro da Transformação Digital da Ucrânia, constituiu um 'Exército de TIC', cujo objetivo principal era travar um contra ataque cibernético contra a Rússia. "Fedorov solicitou a assistência de um especialista cibernético e *twittou* um Telegram com uma lista de 31 sites-alvo de empresas e organizações estatais russas" (Pagliusi, 2022, op. cit). "O canal Telegram listou os sites de 31 grandes empresas e organizações estatais russas, incluindo a gigante de energia Gazprom, o segundo maior produtor de petróleo da Rússia, Lukoil, três bancos e um punhado de sites governamentais" (Pearson, J., 2022, 27 de fevereiro). O autor divulgou ainda que o site oficial do Kremlin, Kremlin.ru, foi colocado offline em um "aparente ataque distribuído de negação de serviço (DDoS)".

Os ciberguerreiros ucranianos combatem a invasão russa sentados à frente dos seus computadores e no país existem mais de 300 mil membros do 'exército *TIC*'[61], alguns hackers estão a desenvolver e disseminar entre as pessoas com menos conhecimentos tecnológicos, softwares mais simples para esses também conseguirem aderir ao exército *TIC* e executar ações contra ofensivas ucranianas.

A Tabela IV do Anexo (p.IV) apresenta a síntese dos principais ataques cibernéticos promovidos pela Ucrânia contra a Rússia, no intervalo entre maio de 2016 e fevereiro de 2022, mencionados nesse capítulo.

3.2 Visão Prospectiva

Concluída a investigação numa conjuntura temporal em que continua em curso o conflito entre a Ucrânia e a Rússia com desenvolvimentos diários, torna-se difícil traçar uma visão prospectiva tanto mais que outros atores internacionais surgiram em cena, de forma mais ou menos assumida. Até o momento, parece não haver perspectiva de um acordo, a curto prazo, de paz entre Ucrânia e Rússia.

[61] Fonte: Visão (2022). Como os hackers na Ucrânia estão a atacar os sites russos, mais uma frente de batalha. Recuperado de: https://visao.sapo.pt/atualidade/mundo/guerra-na-ucrania/2022-03-22-como-os-hackers-na-ucrania-estao-a-atacar-os-sites-russos-mais-uma-frente-de-batalha/ (Em 19/10/2022)

Conflitos como esse não se resumem a tiros, bombas, drones, mísseis, tanques a avançar por terra, a ataques aéreos e marítimos, pois farão sempre parte de uma guerra híbrida, através de interferência política, direta e indireta, da guerra da informação, através da disseminação em massa de fake news, da influência em campanhas eleitorais, da interferência das relações políticas, económicas e diplomáticas e da promoção de ciberataques com o objetivo de enfraquecer o adversário. A utilização em larga escala das redes sociais com o objetivo de manipular as pessoas, disseminar desinformação, para gerar desestabilização, desconfiança, descontentamento e revolta, promete ser uma prática cada vez mais utilizada e a vitória final estará relacionada em maior grau a ações mais subtis e discretas.

É possível admitir que já vivemos o período denominado de 'Nova Guerra Fria' cibernética, híbrida, assimétrica e global em que o conflito já não é travado apenas a uma escala regional se for tida em conta, sobretudo, a origem do elemento tecnológico presente no cenário diário no ciberespaço, onde não se pode atuar de forma amadora ou voluntarista. É incontestável afirmar que o elemento cibernético vai intensificar-se, já não sendo possível que os Estados fiquem à margem do processo de transformação digital a nível mundial, acelerado fortemente pela pandemia da Covid 19.

Diante dessa nova realidade, cada Estado deverá constituir o seu exército cibernético, com estatuto idêntico ao das outras Forças Armadas, que tenha o seu próprio orçamento de defesa, com cibercombatentes especializados e doutrinados em táticas de combate no ciberespaço, onde o tempo de resposta é completamente diferente dos outros domínios em que uma ofensiva pode durar dias, meses e até anos.

Diante desse cenário, caso um país-membro da NATO seja alvo de um ataque cibernético, que cause perda de vidas ou danos irreparáveis, isso pode vir a invocar o Artigo 5º do tratado, a cláusula de defesa coletiva da aliança. Esse seria um enorme revés, já que desencadearia uma guerra na qual a NATO teria que aderir. O caso mais provável é que, inicialmente, os contra-ataques partam diretamente dos EUA e de aliados próximos.

Os Estados Unidos têm pressionado a União Europeia a manter as sanções aplicadas à Rússia de maneira que a Europa deixe de comprar o gás e o petróleo russos, base do desenvolvimento europeu, passando a ter que comprar o americano a um preço

mais caro, o que atende à promessa de campanha de Joe Biden, quanto à recuperação da indústria petrolífera americana[62].

Como afirmou John Foster Dulles "Não há países amigos, mas interesses comuns", dessa forma, a China vem aproximando-se da Rússia, com o objetivo de negociar a seu favor a produção excedente da energia fóssil, o petróleo e o gás baratos, e passou a ser o seu maior cliente, situação que permitiu à China ditar o valor de compra. Quanto mais a Rússia precisar do apoio de Pequim para continuar a guerra contra a Ucrânia melhor para a China porque continuará a comprar o petróleo e o gás cada vez mais baratos o que impulsionará ainda mais a sua economia e permitirá reforçar a sua posição em relação aos Estados Unidos[63].

Uma nova Ordem Mundial está a ser construída nesse momento, paralelamente à guerra híbrida entre Rússia e Ucrânia, enquanto o mundo se distrai com muitos outros fatos, aparentemente menos relevantes, que estão a ocorrer na cena mundial, simultaneamente a tantos acontecimentos que dividem as atenções da comunicação social. Alguns atores já perceberam a aproximação do fim da hegemonia americana e a dimensão da crescente ameaça da implantação de uma nova ordem mundial, baseada em regras no Indo-Pacífico, ou até de um mundo de Múltiplas Ordens, (Pinto, 2023). A Austrália, por exemplo, já revelou uma mudança radical em seu orçamento de Defesa, e seu primeiro-ministro Anthony Albanese anunciou "Não podemos cair em velhas suposições. Devemos construir e fortalecer nossa segurança procurando moldar o futuro em vez de esperar que o futuro nos molde"[64].

[62] The White House: President Biden Announces Release from the Strategic Petroleum Reserve As Part of Ongoing Efforts to Lower Prices and Address Lack of Supply Around the World https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/23/president-biden-announces-release-from-the-strategic-petroleum-reserve-as-part-of-ongoing-efforts-to-lower-prices-and-address-lack-of-supply-around-the-world/ (em: 23.11.21).

[63] Reuters: Putin says Russia now one of China's leading oil and gas suppliers. https://www.reuters.com/business/energy/putin-says-russia-now-one-chinas-leading-oil-gas-suppliers-2022-12-30/ (em: 30.12.2022).

[64] Whitemann, H. (04/2023): De olho na China, Austrália anuncia maior reforma militar desde a Segunda Guerra. Recuperado de: https://www.cnnbrasil.com.br/internacional/de-olho-na-china-australia-anuncia-maior-reforma-militar-desde-a-segunda-guerra/

Conclusão

Terminada a análise, cumpre destacar as principais conclusões. O objetivo que levou à elaboração dessa dissertação consistia no reconhecimento da relevância do ciberterrorismo e sua importância relativamente a uma Nova Guerra Fria.

A investigação iniciou-se pelo enquadramento conceptual-histórico do terrorismo no qual foi possível observar definições diferentes por parte de diversos autores. Por ser uma temática complexa, extensa e abrangente que se pode referir a uma tática, um ato anarquista, criminoso, com motivações políticas, religiosas ou ideológicas, existem inúmeras definições para a palavra terrorismo, importando referir que se trata de um "fenómeno quase tão antigo como o homem, embora ao longo da História tenha conhecido múltiplas facetas" (Pinto, 2018, p. 11).

Verificou-se que o terrorismo contemporâneo, mais especificamente a partir de 2001, ano em que a Al Qaeda levou a cabo os ataques nos Estados Unidos, o 11 de Setembro de 2001, influenciou os modelos de segurança, no sentido da compreensão da ameaça focada na Segurança Nacional dos Estados na guerra contra o terrorismo. Buzan & Hansen (2010) em *The Evolution of International Security Studies* contribuem grandemente para a compreensão do conceito de segurança no período pós-11 de Setembro e discutem os elementos securitários existentes na época e a necessidade da expansão do conceito de segurança internacional na guerra contra o terrorismo.

Verificou-se também que não há uma única conceptualização de Terrorismo de Estado, no âmbito das Relações Internacionais, das organizações intergovernamentais ou empresariais. Confrontar esta modalidade do terrorismo, indubitavelmente leva a debates intermináveis e intensos, principalmente no que se refere ao Ciberterrorismo, cuja ação dificilmente se consegue atribuir a um Estado, havendo divergências quanto à atribuição do status de "Estados Terroristas", aos Estados que violam leis internacionais e causam danos colaterais incomensuráveis no espaço virtual,

À semelhança do conceito da globalização o terrorismo global refere-se ao terrorismo transnacional por meio do qual atores violentos não estatais atuam em vários territórios, cujos atos são difíceis de prever e monitorizar, e cuja atividade foi facilitada com a globalização e a internet, alargando o campo de atuação terrorista, que passou a ser orquestrado, de diversas formas, no ciberespaço.

Em resposta à primeira pergunta de partida – 1. O que é ciberterrorismo? - embora não exista um conceito universal sobre o tema, Denning (1999, p. 241) define-o como "a convergência entre o ciberespaço e o terrorismo. São ataques ilegais contra os computadores, redes e as informações neles armazenadas, efetuados para intimidar ou coagir um Governo ou o seu povo, em prol de objetivos políticos ou sociais". De forma mais abrangente é possível afirmar que a guerra cibernética desempenha um papel importante no mundo moderno e trata-se de uma atividade de suma importância, de modo que todas as potências militares mundiais já criaram unidades e agências especiais dedicadas a ela. A guerra cibernética envolve duas frentes importantes, a espionagem e a sabotagem, que vão desde a destruição de projetos e documentos até ações diretas contra infraestruturas controladas por computadores.

Relativamente à segunda pergunta de partida – 2. Qual e a verdadeira dimensão da ameaça do ciberterrorismo? - segundo Clarke, R. & Knake, R. (2015) "todo o fenómeno da guerra cibernética é de tal forma cercado de sigilo governamental que faz os tempos da Guerra Fria parecerem uma época de transparência e abertura". Trata-se atualmente da arma mais poderosa desejada por todos os exércitos do mundo. Observa-se que atualmente existam entre 20 a 30 países conhecidos por terem unidades de guerra cibernética qualificadas, além dos Estados Unidos e Rússia, que são os países com maior destaque. Não se sabe exatamente o total do montante que cada país dedica para o desenvolvimento dessa área, mas estima-se que sejam valores muito elevados que crescem a cada ano. No que se refere às grandes potências, haverá sempre a pretensão de dominarem estrategicamente o ciberespaço e terem uma posição de vantagem em relação aos seus adversários na guerra cibernética, no entanto, a sua própria dependência do ciberespaço torna-se também a sua maior vulnerabilidade. Dito isto, é verdadeiro afirmar que a dimensão do poder nesse âmbito é proporcional ao tamanho da vulnerabilidade dos atores envolvidos.

Como é sabido, muitos países não possuem planos concretos e eficazes de segurança cibernética para proteger as suas infraestruturas críticas e, como tal, estão mais suscetíveis aos ataques. Por isso, é de suma importância que os governos e empresas invistam no desenvolvimento e implementação de estratégias que visem a restrição dos riscos para as suas infraestruturas críticas. Ao longo do trabalho foram abordados alguns casos emblemáticos de forma a perceber a verdadeira dimensão das novas ameaças.

De forma a responder à terceira pergunta de partida – 3. A guerra no domínio cibernético pode ser configurada como a Nova Guerra Fria? - Paglisui (2022)[65] chamou a atenção para a necessidade de perceber que a militarização do ciberespaço irrompe como "o quinto domínio da guerra – após o terrestre, marítimo, aéreo e geoespacial", onde vêm sendo travados combates já há tempos, entre nações tecnologicamente mais avançadas, "por meio de um novo tipo encoberto de guerra: a Guerra Fria Cibernética"[66]. O mesmo autor também afirma que esse novo tipo de combate "abrange desde ações dissimuladas de coleta de inteligência via meio digital, até a interrupção de serviços online" visando bloquear *sites* de sistemas financeiros, logísticos, de geolocalização e de atendimento público governamental, além da "disrupção de infraestruturas críticas do oponente, sejam civis ou militares". Face ao exposto, constata-se que os ataques cibernéticos constituem uma preocupação crescente para as grandes potências. Daí a sua aposta ou investimento na procura de cibersegurança. Um desiderato nem sempre atingido.

A investigação e recolha documental para elaboração dessa dissertação, permite apresentar algumas conclusões epistemológicas que aponta, para que o ciberterrorismo seja uma revisitação da época em que o mundo vivia uma Guerra Fria porque neste conflito não se verifica apenas o uso dos recursos tradicionais de guerra e, por isso, a invasão russa da Ucrânia corresponde a uma nova dimensão do poder nas Relações Internacionais e que irá condicionar a construção de uma Nova Ordem Mundial. Contudo, importa dizer que a resposta do Ocidente ao ciberterrorismo baseia-se, sobretudo, numa estratégia de defesa, já que a opinião pública dos Estados democráticos jamais aceitaria que o ciberterrorismo fosse combatido na mesma moeda. Nesse sentido, o Ocidente organiza-se de forma a criar órgãos e mecanismos que falem entre si e permitam desmantelar as redes internacionais de ciberterrorismo, que, por sua vez, praticam cada vez mais ações ofensivas.

Em relação ao cenário mundial, esta investigação conclui que o mundo está de fato a assistir ao surgimento de uma revisitação do clima de Guerra Fria, mas, simultaneamente, à construção de uma nova dinâmica na Ordem Mundial, em que o Ciberterrorismo desempenha o papel principal. Tal como Moreira (2019, p. 12) afirmou

[65] Paglisusi, P. (2022). Guerra Cibernética Russo-Ucraniana – Lições para o Brasil e o Mundo. Recuperado em: 24/05/2022 em: https://www.sitedaseguranca.com.br/2022/05/02/guerra-cibernetica-russo-ucraniana-licoes-para-o-brasil-e-o-mundo/

[66] Pagliusi, P., op. cit

"hoje o problema essencial é assumir que o «poder de destruir o planeta» está pendente, como talvez repetisse Bismark, de uma simples leviandade".

Segundo Raymond Aron, a guerra fria foi definida como um período de paz impossível e de guerra improvável. No contexto da guerra Russo-Ucraniana, marcado por crescentes combates no ciberespaço, que levou ao conflito armado para recuperação de território, com envolvimento estrangeiro, pelo menos em termos de fornecimento de material bélico, de treinamento militar e de inteligência, o mundo está a assistir ao surgimento de uma nova modalidade de guerra com componentes: híbridos, encobertos, dissimulados, a denominada "Nova Guerra Fria", que está a ocorrer simultaneamente à construção de uma nova dinâmica na ordem mundial, em que o ciberterrorismo será predominante. Diante de tudo isso, parece correto afirmar que, a soberania no 5º domínio da guerra representará um elemento crítico na construção da Nova Ordem Mundial para a qual temos que nos preparar.

A partir desta dissertação e no âmbito de investigações futuras, com base em estudos mais alargados e aprofundados sobre cibersegurança, respectivamente no que tange à Diplomacia e as Relações Internacionais, seria interessante redefinir as habilidades dos atuais e futuros Diplomatas, uma vez que estes deverão estar capacitados e bem assessorados para lidar com os conflitos no 5º domínio e, consequentemente, preparados negociar perante as novas ameaças.

Bibliografia

Amaresh, P. (2020). *The Art of War- Chinas Sharp Power Strategy*, p.2. Recuperado de: https://www.academia.edu/44608938/The_Art_of_War_China_s_Sharp_Power_Strategy_2020_ (em 18/01/2022)

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming. *Comparative Strategy*, p.p. 141–165.

Barboza, C. (2018). *A Estratégia Russa no Conflito da Ucrânia: contribuições para a doutrina militar brasileira.* Escola de Comando e Estado Maior do Exército Escola Marechal. Rio de Janeiro. Recuperado de: file:///G:/Meu%20Drive/Lus%C3%B3fona/Disserta%C3%A7%C3%A3o/Textos%20&%20Fontes/MO%205965%20-%20MATOS%20BARBOZA.pdf. Em 16/10/2022.

Benedictus, L. (2016). Invasion of the troll armies: from Russian Trump supporters to Turkish state stooges. *The Guardian*. Recuperado de: https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian (Em: 03/11/2022)

Bianchi, A. (2004). *Enforcing International Law Norms Against Terrorism.* Oxford and Portland Oregon: Hart Publishing (p. vi).

Blank, S. (2017). Cyber War And Information War À La Russe. In: Perkovich, George; Levite, Ariel E. *Understanding Ciber Conflict: Fourteen Analogies*. Georgetown: Georgetown University Press.

Borum, R. (2017). The Etiology of Radicalization, In: LaFree, G. & Freilich, J.D. (Eds.) *The Handbook of Criminology of Terrorism*, p.p. 17-32, USA: Wiley Blackwell

Bravo, R. (2011). Do espectro de conflitualidade nas redes de informação: Por uma reconstrução conceptual do terrorismo no ciberespaço. *Investigação Criminal*, 2, p.p. 174-200.

Breeden, A.; Chan, S.; Perloth, N. (2017): Macron Campaign Says It Was Target of 'Massive' Hacking Attack. *The New York Times.* Recuperado de: https://www.nytimes.com/2017/05/05/world/europe/france-macron-hacking.html (Em: 07/07/2022).

Butler, P. (2002). Terrorism and utilitarianism: Lessons from and for, criminal Law. *Journal of Criminal Law and Criminology*, 93, p.p. 1-22.

Buzan, Barry & Hansen, Lene. (2010). *The evolution of International security studies*. Cambridge: Cambridge University Press.

Carrapico, H., & Barrinha, A. (2018). *European Politics and Society European Union cyber security as an emerging research and policy field*. https://doi.org/10.1080/23745118.2018.1430712

Cavelty, M. (2010). Cyber-threats. In *The Routledge Handbook of Scurity Sctudies* (pp. 180–189). Londres.

Chai, W.(s.d.): Five Eyes Alliance. https://www.techtarget.com/whatis/definition/Five-Eyes-Alliance (em 08.03.2022)

Chaves, A. & Arguelhes, D. (2014). Guerra Fria: Uma leitura da formação de aspectos conceituais. *OPSIS*, Catalão-GO, v. 14, n. Especial. p.p. 137.

Clarke, R. & Knake, R. (2015). *Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito.* Rio de Janeiro: Brasport.

Clausewitz, C. Von. (2014). *Da Guerra.* São Paulo: Martins Fontes

Cohen, S. B. (2015). *Geopolitics: the geography of international relations.* 3. ed. Londres: Row-man & Littlefield.

Cole, M. (2017). Top-Secret NSA Report Details Russian Hacking Effort Days before 2016 Election. *The Intercept*, 5 de junho. Disponível em: https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/, (Recuperado em: 07/07/2022).

Conselho da Europa (2017). Convenção Europeia para eliminação do Terrorismo, Estrasburgo, 27-1-1977. Disponível em http://conventions.coe.int/Treaty/en/Treaties/html/090.htm, (Recuperado em: 0/12/2021).

Denning, D. (1999, p. 1-4). *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, Global Problem Information Technology and Tools.* Disponível em: https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/, (Recuperado em: 13/12/2021).

Denning, D. (2000) *Cyberterrorism: The Logic Bomb versus the Truck Bomb*. Online:

https://www.proquest.com/openview/630686bfa511184f2ee33a00ea8caeac/1?pq-origsite=gscholar&cbl=55193 , (Recuperado em: 12/12/2021).

Diário da República Eletrônico: Lei n.º 52/2003, de 22 de agosto. https://dre.pt/dre/detalhe/lei/52-2003-656128 (em: 22.06.2022).

Diário de Notícias: Governo iraniano impõe restrições ao uso de internet. https://www.dn.pt/internacional/governo-iraniano-impoe-restricoes-ao-uso-de-internet-15374517.html (em: 21.11.2022).

Doward, J. (2017). Malta accuses Russia of cyber-attacks in run-up to election. *The Guardian*. 27 de maio. Disponível em: https://www.theguardian.com/world/2017/may/27/russia-behind-cyber-attacks-says-malta-jseph-muscat, (Recuperado em: 07/07/2022).

Dupuy, P.M. (2004). "State Sponsors of Terrorism: Issus of Responsibility", in: BIANCHI, Andrea (Ed.), *Enforcing International Law Norms against Terrorism*. Portland: Hart; p. 5.

Eurodefense Portugal. A Evolução da Guerra e a 2ª invasão da Ucrânia. https://eurodefense.pt/a-evolucao-da-guerra-e-a-2a-invasao-da-ucrania/ (em: 21.11.2022).

European Comission (2016). *Racism and Intolerance General Policy Recommendation 15 on combating Hate Speech*. Strasbourg: ECRI Secretariat, Directorate General of Democracy, Council of Europe.

Fernandes, J. (2019). *Geopolítica em Tempo de Paz e Guerra*. Coimbra. Almedina: p. 164.

Flore, M. et al. (2019). Understanding Citizens' Vulnerabilities To Disinformation And Data-Driven Propaganda. Eur 29741 En, *Publications Office Of The EuropeanUnion*, Luxemburgo. https://publications.jrc.ec.europa.eu/repository/handle/JRC116009, (Recuperado em: 31/05/2022).

Freitas, P. (2022, pp. 115-130): Ciberterrorismo e a Lei de Combate ao Terrorismo. https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD161/NeDef161_6_PedroMiguelFreitas.pdf. (em: 22.06.2022).

Gaspar, C. (1998). A Rússia e a segurança europeia. *Nação e Defesa*, Lisboa, Inverno 98 N° 84 - 2. a Série. Recuperado de: https://comum.rcaap.pt/bitstream/10400.26/1532/1/NeD084_CarlosGaspar.pdf>. (Recuperado em: 02/06/2022).

Geeks, K. (2015). *Cyber War in Perspective Russian Agression against Ukraine*, NATO Cooperative Cyber Defence Centre of Excellence, Tallin, Estônia.

Giles, K. (2012). Russian cyber security: concepts and current activity. *Conflict Studies Research Centre–Chatham House*, p.p. 1-3.

Gorbachev, M. (1991). *O golpe de agosto*: *a verdade e as lições.* Tradução de Regina Amarante. São Paulo: Best Seller.

Hagelstam, A., Narinen, K. (2018). *Cooperating to counter hybrid threats*.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), p.p. 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hogan, M. & Paterson, Th. (1991). *Explaining American foreign relations*. New York; Cambridge University Press.

Iasakova, E. (2019). *Владимир Путин Подписал Закон О Рунете* [Vladimir Putin Assinou Lei Sobre A Runet]. Rossiyskaia Gazeta. Disponível Em: Https://Rg.Ru/2019/05/01/Vladimir-Putin-Podpisal-Zakon-O-Runete.Html, (Recuperado em: 13/06/2022).

IGES(Institute for Geopolitics, Economy and Security). Mackinder: Who rules Eastern Europe rules the World. https://iges.ba/en/geopolitics/mackinder-who-rules-eastern-europe-rules-the-world/(em: 21/11/2022)

Inform Napalm. https://informnapalm.org/en/tag/ukraine/ (em: 19.10.2022)

Informe Napalm (2022). *Um Portal que une os esforços de mais de 30 voluntários de mais de 10 países cujas investigações estão disponíveis para os leitores em mais de 20 idiomas.* Recuperado de: https://informnapalm-org.translate.goog/en/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=wapp (Em: 04/11/2022).

Insight Report (2023). Global Cybersecirity Outlook 2023. https://www.weforum.org/reports/global-cybersecurity-outlook-2023/ (em: 08.05.202)

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38* (2), p.p. 7-40. Recuperado de: https://direct.mit.edu/isec/article/38/2/7/12094/The-Meaning-of-the-Cyber-Revolution-Perils-to, (Recuperado em: 03/11/2022).

Kissinger, H. (2017). *A Ordem Mundial*. 4ª. Ed. Portugal: Dom Quixote, p. 419

Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O., & Oberholtzer, J. (2017). *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. Recuperado de: https://www.rand.org/pubs/research_reports/RR1498.html (Recuperado em 16/10202).

Kramer, A. E. (2022). Hackers derrubam sites do governo na Ucrânia. *The New York Times* . https://www-nytimes-com.translate.goog/2022/01/14/world/europe/hackers-ukraine-government-sites.html?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=wapp, (Recuperado em: 19/10/2022).

Lara, A. & Al (2014). *Crise, Estado e Segurança*. Edições MGI, Lisboa, p. 25

Leal, F. (2017). *História do Terrorismo: Da Antiguidade à Alcaida*. https://www.academia.edu/34400890/Hist%C3%B3ria_do_Terrorismo, (Recuperado em: 07/10/2021).

Lew, J. & Roughead, G (dir.) (2021). China's Belt and Road:*Implications for the United States.* https://www.cfr.org/task-force-report/chinas-belt-and-road-implications-for-the-united-states/ (Recuperado em: 14/11/2022).

Lia. B. (2008). Architect of Global Jihad: The Life of Al-Qaeda Strategist Abu Mus´ab al Suri. *New York: Columbia University Press* (pp. 18-19).

Limnel, J. (2015). The Exploitation of Cyber Domain as Part of Warfare: Russo-krainian War. *International Journal of Cyber-Security and Digital Forensics*, vol 4, p.521- 532

MacMahon, R. J. (2012). Guerra Fria. https://www.lpm.com.br/livros/Imagens/guerra_fria_encyclopaedia_trecho.pdf, (Recuperado em: 29/09/2021).

Marthoz, JP. (p. 202018). *Terrorismo e a mídia: um manual para jornalistas*. Brasília

Matusitz, J. (2013). *Terrorism & Communication: A Critical Introduction*. Sage Publications Inc. California, p. 415

Maynard, D. (2018). Considerações Sobre A Ciberguerra. In: Silva, Francisco CarlosTeixeira Da & Schurster, Karl (Org.). *Por Que A Guerra?* Rio De Janeiro: Civilização Brasileira.

Moreira, A. (1997). *Teoria das Relações Internacionais*, 2.ª Edição, Livraria Almedina, Coimbra, p. 47.

Moreira, A. (2001). *Ciência Política*. Coimbra: Almedina (p. 190)

Moreira, A. (2019). *A Nossa Época - Salvar a Esperança*. 1ª Edição, Edições Sílabo, Lisboa, p. 13.

National Counterterrorism Center. Presidential Document: Executive Order 13354 of August 27, 2004. https://www.govinfo.gov/content/pkg/FR-2004-09-01/pdf/04-20050.pdf (em: 15.12.2022)

NATO (2016). *The Secretary General´s Annual Report* 2016. Brussels: NATO Public Diplomacy Division.

NATO Review [online]. Disponível em: https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html (Recuperado em: 12/12/2022).

Nunes, P. V (2015). *Sociedade em Rede, Ciberespaço e Guerra de Informação – Contributos para o enquadramento e Construção de uma Estratégia Nacional de Informação*, Lisboa: Instituto da Defesa Nacional, p. 142.

Nye, S. N. Jr (2004). *Soft Power: The Means to Success in World Politics*.

Oksana,M. Chernysh, N. et Susak, V. (2016, p. 6). *Forced choice: identities and attitudes before and aer Euromaidan. Ukranian Socie*ty. Recuperado de: file:///C:/Users/Lilian/Downloads/Forced%20choice%20identities%20and%20attitudes%20before%20and%20after%20Euromaidan%20-%20en.pdf, (Recuperado em: 02/06/2022).

Osterweil, E., Stavrou, A. & Zhang, L. (2019). *20 Years of DDoS: a Call to Action.* [S.l.]: Vol. 1, Artigo 1º, publicado em abril de 2019, pp. 1-11.

Pagliusi, P. (2022). *Geopolítica: Guerra Cibernética e Segurança da Informação. Webinário.* Liga da Defesa Nacional – Diretoria Estadual do Rio de Janeiro. Recuperado de: https://ldn-rj.org/geopolitica-guerra-cibernetica-e-seguranca-da-informacao/ (Em 12/10/2022).

Pagliusi, P. (2022). *Guerra Cibernética Russo-Ucraniana – Lições para o Brasil e o Mundo.* http://www.pagliusi.com.br/2022/03/guerra-cibernetica-russo-ucraniana.html, (Recuperado em: 18/10/2022)

Pearson, J. (2022). "*Ucrânia lança 'exército de TI' e mira no ciberespaço russo*" . Reuters. Recuperado de:https://www-reuters-com.translate.goog/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=wapp (Em: 19/10/2022).

Pedahzur, A. & Martin, S. (2017). Evolution of Suicide Attacks, In: LaFree, G. & Freilich, J.D. (Eds.) *The Handbook of the Criminology of Terrorism*, USA: Wiley Blackwell, (pp. 339-352).

Phillips, A. (2010). Trasnational Terrorism. In Beeson, Mark & Bisley, Nick (Eds.) Issues in *21st Century World Politics, Basingstoke: Palgrave* Macmillan. (p. 139)

Pinto, J. (2023). O Fim da Hegemonia Americana: Um Mundo de Múltiplas Ordens. Lisboa. Edições Sílabo Lda. 1º Edição

Pop-Eleches, G & Robertson, G. (2018, pp. 108-117). Identity and political preferences in *Ukraine – before and after the Euromaidan. Post-Soviet Affairs, Princeton.* Recuperado de: https://doi.org/10.1080/1060586X.2018.1452181. (Em: 02/06/2022)

Ramos, T. (2019) *A operação de ocupação da Crimeia*. Academia Militar. Lisboa. Recuperado de: https://1library.org/document/zp25k7vy-analise-da-intervencao-russa-na-crimeia.html. (Em: 16/10/2022)

Rapoport, D. (2002). *The four waves of rebel terror and September 11.* USA. Antthropoetics, (p.8)

Rato, V. (2020). *De Mao a Xi.* Lisboa: Alethéa, p.174.

Reuters: Putin says Russia now one of China's leading oil and gas suppliers. https://www.reuters.com/business/energy/putin-says-russia-now-one-chinas-leading-oil-gas-suppliers-2022-12-30/ (em: 30.12.2022).

Rutenberg, J. RT, (2017). Sputnik and Russia's New Theory of War. *The New York Times Magazine*. https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html, (Recuperado em: 27/08/2022).

Sanger, D. E. (2018).*The Perfect Weapon: War Sabotage And Fear In The Cyber Age*. New York: Crown

Santana, V. (2020). *A lavagem de dinheiro por meio de criptomoedas e o risco para defesa nacional, p. 5.*, Recuperado de: https://repositorio.esg.br/bitstream/123456789/969/1/VINICIUS%20SANTANA%20-%20TCC%20CAED%202020%20v2.pdf (Em: 11/07/2022)

Sawyer, R. (2010). *A Arte da Guerra*. 2ª. Tiragem. São Paulo: Brasil. WMF Martins Dontes Ltda. (p. 40)

Schwirtz, M. (2017). "German Election Mystery: Why No Russian Meddling?". *The New York Times*, 21 de setembro. Disponível em: https://www.nytimes.com/2017/09/21/world/europe/german-election-russia.html., (Recuperado em: 07/07/2022).

Shandra, A.& Seely, R. (2019). *The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine*. Recuperado de: https://rusi.org/explore-our-

research/publications/occasional-papers/surkov-leaks-inner-workings-russias-hybrid-war-ukraine (Em: 19/10/2022).

Snowden Archive: https://theintercept.com/collections/snowden-archive/ (em 08.03.2022)

Stowell, J. (2018). "*What is Hybrid Warfare*?". Global Security Review. Disponível em: https: //globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war), Recuperado em: 19/10/22).

Suzuki, S. (2022). *A guerra cibernética paralela entre Rússia e Ucrânia*. BBC News Brasil, Sao Paulo. Recuperado de: https://www.bbc.com/portuguese/internacional-60551648 (em: 12/10/2022).

The Epic Turla (snake/Uroburos) attacks. https://www.kaspersky.com/resource-center/threats/epic-turla-snake-malware-attacks. (em 12.10.2022)

The White House: President Biden Announces Release from the Strategic Petroleum Reserve As Part of Ongoing Efforts to Lower Prices and Address Lack of Supply Around the World https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/23/president-biden-announces-release-from-the-strategic-petroleum-reserve-as-part-of-ongoing-efforts-to-lower-prices-and-address-lack-of-supply-around-the-world/ (em: 23.11.21).

Tuptuk, N. & Hailes, S. (2016). The cyberattack on Ukraine's power grid is a warning of what's to come. *PHYSORG*. Recuperado de: https://theconversation.com/the-cyberattack-on-ukraines-power-grid-is-a-warning-of-whats-to-come-52832 (Em: 04/11/2022).

Ukranian Cyber Alliance. https://cyber.org.ua/ (em: 19.10.2022).

UNESCO (2018). *Organização das Nações Unidas para a Educação, a Ciência e a Cultura.* SP, France e a Representação da UNESCO no Brasil.

Ventura, J.; & Carvalho, C., (2020). *Da Radicalização Ideológica ao Terrorismo: Uma digressão*. Lisboa: Diário de Bordo, p. 165.

Ventura, J.; & Carvalho, C., (2020). *Da Radicalização Ideológica ao Terrorismo: Uma digressão*. Lisboa: Diário de Bordo, p. 64.

Visacro, A. (2018). *A Guerra na Era da Informação*. S. Paulo, Brasil: Contexto.

Visão (2022). *Como os hackers na Ucrânia estão a atacar os sites russos, mais uma frente de batalha*. Recuperado de: https://visao.sapo.pt/atualidade/mundo/guerra-na-ucrania/2022-03-22-como-os-hackers-na-ucrania-estao-a-atacar-os-sites-russos-mais-uma-frente-de-batalha/ (Em: 04/11/2022).

Visão (2022). Como os hackers na Ucrânia estão a atacar os sites russos, mais uma frente de batalha. Recuperado de: https://visao.sapo.pt/atualidade/mundo/guerra-

na-ucrania/2022-03-22-como-os-hackers-na-ucrania-estao-a-atacar-os-sites-russos-mais-uma-frente-de-batalha/ (Em 19/10/2022)

Warsau Institute (2017). *Donbass Leaks*. Recuperado de: https://warsawinstitute.org/donbass-leaks/ (Em: 19/10/2022).

Weedon, J. (2015): Beyond Cyber War: Russia´s use of Strategic Cyber Espionage and Information Operations in Ukraine. In: Geers, K (ed.*). Cyber War in Perspective: Russian Aggression Against Ukraine*. p.p. 67-77, NATO CCDCOE Publications. Tallinn.

Weimann, G. (2012). Lone Wolves in Cyberspace. *Journal of Terrorism Research*, vol. 3, Issue 2. The Centre of the Study of Terrorism and Political Violence (p.p. 75-90)

Whitemann, H. (04/2023): De olho na China, Austrália anuncia maior reforma militar desde a Segunda Guerra. Recuperado de: https://www.cnnbrasil.com.br/internacional/de-olho-na-china-australia-anuncia-maior-reforma-militar-desde-a-segunda-guerra/

Anexos

Tabela I

Panorama das Ameaças de 2021 elaborado pela ENISA
(Agência de Cibersegurança da União Europeia):

Ransomware	Tipo de ataque malicioso em que os cibercriminosos cifram os dados de uma organização e exigem pagamento para lhe devolverem o acesso.
Malware	*Software* malicioso concebido com a intenção de aceder a um dispositivo sem autorização ou de o danificar ou comprometer.
Criptossequestro (Cryptojacking)	Uso não autorizado de computadores, telemóveis inteligentes e tábletes alheios para gerar criptomoeda. A criptomoeda continua a ser o método de pagamento mais comum entre os criminosos.
Ataques por mensagem eletrônica	Tentativas de roubo de senhas e palavras-passe ou dados de cartões de crédito com recurso a várias técnicas (p. ex. ciberiscagem, ciberiscagem por SMS e correio eletrónico não solicitado).
Violação de dados e fugas de informação	Divulgação de dados sensíveis, confidenciais ou protegidos para um ambiente que não seja de confiança.
Ataques distribuídos de negação de serviço (*DDoS*)	Ataques que impedem os utilizadores de uma rede ou sistema de acederem a informações, serviços e outros recursos pertinentes.
Desinformação	Ataque intencional que passa por criar ou partilhar informações falsas e enganadoras para manipular a opinião pública.
Ameaças não maliciosas	Ameaças provocadas sobretudo por erro humano, mas que também podem resultar de catástrofes físicas que causem danos na infraestrutura informática. 50 % dos ataques devem-se a erros de configuração.
Ataques à cadeia de abastecimento	Estratégia de ataque que visa determinada organização explorando vulnerabilidades na sua cadeia de abastecimento que tenham o potencial de gerar um efeito de catadupa. 58 % dos ataques à cadeia de abastecimento têm por objetivo obter acesso a informações.

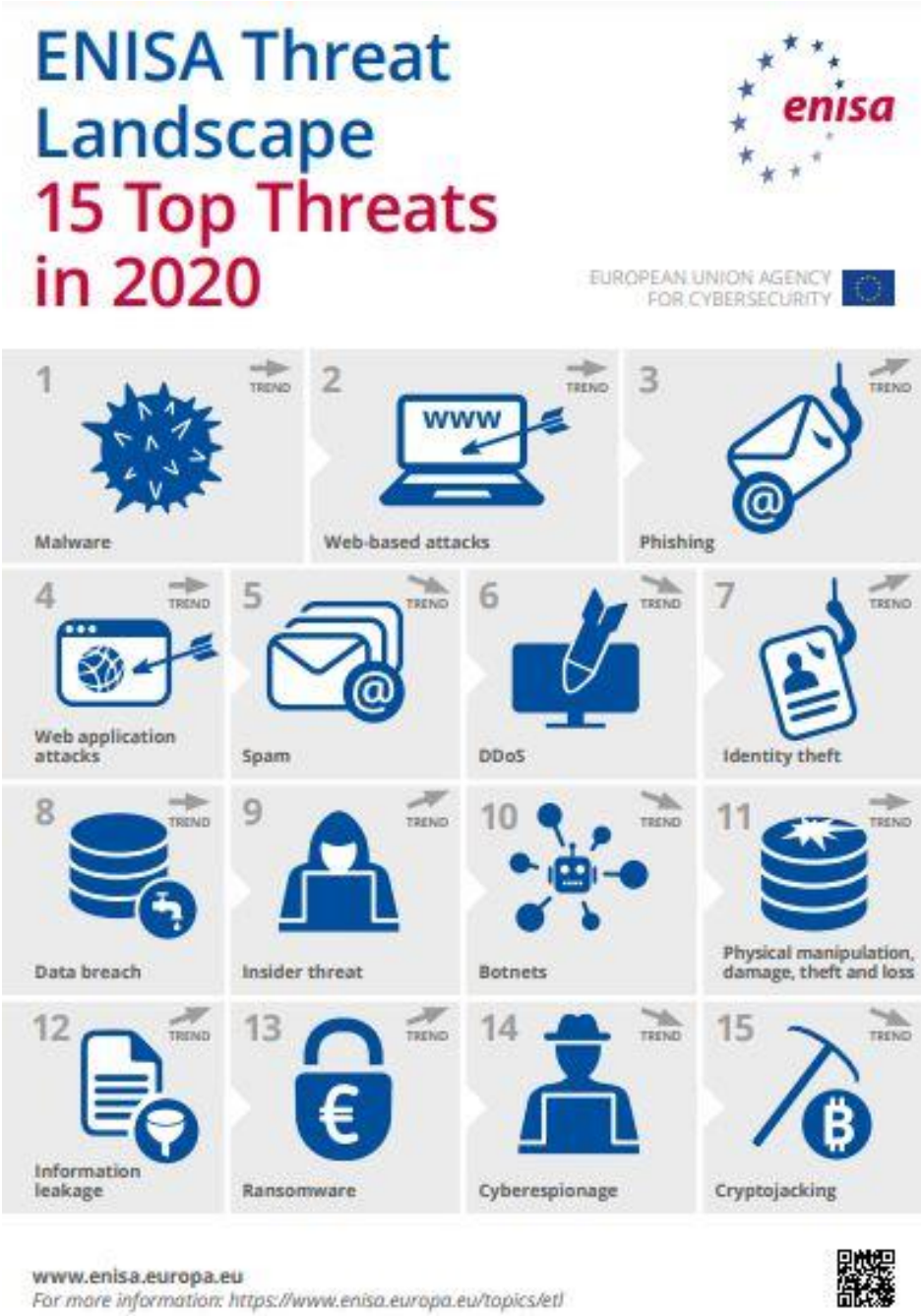
Fonte: Adaptado de Conselho da União Europeia - Principais ciberameaças na EU

(dados de abril de 2020 a julho de 2021)

https://www.consilium.europa.eu/pt/infographics/cyber-threats-eu/ (Recuperado em 16.06.2022)

Tabela II

As 15 Principais ameaças em 2020, segundo a ENISA:



Fonte:https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats Recuperado em 21.08.2022.

Tabela III

Síntese dos principais ciberataques russos contra a Ucrânia no período de 2013 até fevereiro de 2022:

Período	Descrição dos Ciberataques Russos contra a Ucrânia
Ao longo de 2013	Operação "Armageddon".
Fevereiro de 2014	Operação "Snake".
Junho de 2014	Ataques ao sistema automatizado de Eleições.
Dezembro de 2015	Ataque à rede elétrica da Ucrânia. Ataques com o Trojan BlackEnergy em empresas de energia na Ucrânia, que fornecem energia às regiões de Kiev, Ivano-Frankivsk e Chernivtsi. Primeiro ataque cibernético bem-sucedido a uma rede elétrica de que se tem notícia.
Dezembro de 2016	Segundo *hacking* na rede elétrica da Ucrânia.
Dezembro de 2016	Paralisia do Tesouro do Estado da Ucrânia.
Junho de 2017	Ataques cibernéticos de 2017 na Ucrânia, incluindo ataque de hackers em massa na cadeia de suprimentos, usando o vírus Petya. Este se tornou o maior ataque de hackers conhecido até então.
Janeiro de 2022	Ataque cibernético na Ucrânia em 2022, em sites do governo ucraniano, um dia após o fracasso das negociações entre EUA-Rússia sobre o futuro da Ucrânia na OTAN.
A partir de fevereiro de 2022	Ataques em massa, após tropas russas invadirem regiões orientais da Ucrânia, derrubando sites governamentais e bancários ucranianos. A inteligência dos EUA os atribui a ciberatacantes russos, embora o governo russo haja negado tal envolvimento.

Fonte: https://www.sitedaseguranca.com.br/2022/05/02/guerra-cibernetica-russo-ucraniana-licoes-para-o-brasil-e-o-mundo/ (Recuperado em 12/12/2022)

Tabela IV

Síntese dos principais ciberataques ucranianos contra a Rússia no período de 2013 até fevereiro de 2022:

Período	Descrição dos Ciberataques Ucranianos contra a Rússia
Maio de 2016	Operação "Prikormka (Groundbait)".
Maio de 2016	Operação "9 de maio de 2016" (9 *hackings* em sites do grupo separatista **República Popular de Donetsk**, em sites russos de propaganda anti-ucraniana e em **empresas militares privadas russas**).
Junho de 2016	Intervalo do "**Channel One**", em que houve hacking do servidor corporativo do canal russo "Channel One", pela **Aliança Cibernética Ucraniana** (dos hackers *FalconsFlame*, *Trinity* e *Rukh8*).
Outubro de 2016	The **Surkov Leaks**, havendo um vazamento de 2.337 e-mails com centenas de anexos sigilosos, que revelam planos para se tomar a Crimeia da Ucrânia e fomentar distúrbios separatistas em Donbas (documentos datados entre setembro de 2013 e dezembro de 2014).
A partir de fevereiro de 2022	"Exército de TIC" da Ucrânia, criado por **Mykhailo Fedorov**, primeiro vice-primeiro-ministro e ministro da Transformação Digital. Esforço iniciado durante a invasão russa da Ucrânia em 2022, com o propósito de travar uma guerra cibernética contra a Rússia. Fedorov solicitou a assistência de um especialista cibernético e twittou um Telegram, com uma lista de 31 sites-alvo de empresas e organizações estatais russas.

Fonte: https://www.sitedaseguranca.com.br/2022/05/02/guerra-cibernetica-russo-ucraniana-licoes-para-o-brasil-e-o-mundo/ (Recuperado em 12/12/2022)