UNIVERSIDADE FEDERAL DO PARANÁ

GISELE TEIXEIRA TOD

ANÁLISE DA JURISDIÇÃO DO TRIBUNAL PENAL INTERNACIONAL SOBRE A OPERAÇÃO CIBERNÉTICA NOTPETYA

CURITIBA

2022

GISELE TEIXEIRA TOD

ANÁLISE DA JURISDIÇÃO DO TRIBUNAL PENAL INTERNACIONAL SOBRE A OPERAÇÃO CIBERNÉTICA NOTPETYA

Artigo apresentado como requisito parcial à conclusão do curso de Direito, Setor de Ciências Jurídicas, Universidade Federal do Paraná.

Orientador: Prof. Rui Carlo Dissenha

CURITIBA

TERMO DE APROVAÇÃO

ANÁLISE DA JURISDIÇÃO DO TRIBUNAL PENAL INTERNACIONAL SOBRE A OPERAÇÃO CIBERNÉTICA NOTPETYA

GISELE TEIXEIRA TOD

Monografia aprovada como requisito parcial para obtenção de Graduação no Curso de Direito, da Faculdade de Direito, Setor de Ciências jurídicas da Universidade Federal do Paraná, pela seguinte banca examinadora:

Rui Carlo Dissenha
Orientador

Coorientador

Larissa Liz Odreski Ramina
1º Membro

Guilherme Brenner Lucchesi
2º Membro

RESUMO

O presente artigo se propõe a responder a seguinte pergunta: tem o Tribunal Penal Internacional (TPI) jurisdição para processar a operação cibernética NotPetya? Para tanto, parte-se da hipótese inicial de que a operação cibernética investigada se enquadra no crime de guerra de dirigir ataques a objetos civis, previsto no art. 8(2)(b)(ii) do Estatuto de Roma. Os referências teóricos utilizados foram precipuamente decisões de tribunais penais internacionais e doutrina pertinente à temática. Primeiramente, realiza-se uma exposição fática da operação cibernética em si e do(s) conflito(s) existente(s) na Ucrânia ao tempo em que foi lançada. Subsequentemente, são apresentados os requisitos jurisdicionais presentes no Estatuto de Roma, passando em seguida a analisar o caso NotPetya à luz de cada um dos requisitos estabelecidos. Ao final, conclui-se que há incerteza jurídica e fática sobre alguns dos elementos materiais do crime do art. 8(2)(b)(ii) no caso, além de divergência no que toca à interpretação da jurisdição territorial do TPI, podendo a resposta ao questionamento inicial ser tanto negativa quanto positiva.

Palavras-chave: Tribunal Penal Internacional; operação cibernética NotPetya; crime de guerra; jurisdição; Ucrânia.

ABSTRACT

This article aims to answer the following question: does the International Criminal Court have jurisdiction to prosecute the NotPetya cyber operation? In order to do so it works on the assumption that said cyber operation fits into the description of art. 8(2)(b)(ii) of the Rome Statute. Case law from international criminal tribunals and literature regarding the subject were used primarily as source material. Firstly, it gives a factual overview of the cyber operation in question and the armed conflict(s) in Ukraine at the time of its launch. Subsequently, it presents the jurisdictional requirements put forth by the Rome Statute and proceeds to analyse the NotPetya case in light of the aforementioned requirements. In the end, it concludes there are factual and legal uncertainties concerning some of the material elements of the crime set in art. 8(2)(b)(ii), that, alongside the different takes on the ICC's territorial jurisdiction, allows the first question proposed to be answered either in the negative or in the affirmative.

Keywords: International Criminal Court; NotPetya cyber operation; war crime; jurisdiction; Ukraine.

SUMÁRIO

1 INTRODUÇÃO. BREVE CONTEXTUALIZAÇÃO DA OPERAÇÃO CIBERNÉTICA NOTPETYA E DO(S) CONFLITO(S) NA UCRÂNIA 7

2 REQUISTOS JURISDICIONAIS 11

3 JURISDIÇÃO TEMPORAL, TERRITORIAL E NACIONAL 12

4 JURISDIÇÃO MATERIAL 15

4.1 CLASSIFICAÇÃO DO(S) CONFLITO(S) ARMADO(S) NO TERRITÓRIO DA UCRÂNIA 15

4.2 NEXO ENTRE A CONDUTA E O(S) CONFLITO(S) ARMADO(S) 19

4.3 EXISTÊNCIA DE UM ATAQUE 20

4.4 STATUS DOS OBJETOS ATACADOS 22

5 CONCLUSÃO 26

REFERÊNCIAS 28

1. INTRODUÇÃO. BREVE CONTEXTUALIZAÇÃO DA OPERAÇÃO CIBERNÉTICA NOTPETYA E DO(S) CONFLITO(S) NA UCRÂNIA

Em 27/06/2017, mais de 12.500 computadores em 64 países foram atingidos pelo que seria conhecido como a operação cibernética NotPetya (MICROSOFT DEFENDER ATP RESEARCH TEAM , 2017). Um *wiper*[1] disfarçado de *ransomware*[2] havia sido inserido em uma atualização do *software*[3] MeDoc (WAKEFIELD, 2017), usado para fins tributários e contábeis sobretudo na Ucrânia (GREENBERG, 2018).

Os computadores que possuíam o *software* executaram automaticamente a atualização, instalando o *wiper* nos dispositivos. Infectada uma máquina, o *wiper* procurava alcançar os computadores da rede local (ligados a uma mesma conexão) se valendo de brechas do sistema Microsoft desatualizados (entre eles, *EternalBlue PsExec, Windows Management Instrumentation (WMI*), e *EternalRomance*) para criptografar todos os arquivos e o próprio sistema do computador. Outras formas de propagação incluíram a utilização de credenciais/senhas de computadores *logados* e arquivos compartilhados para atingir outros da mesma rede (FAYI, 2018, p. 93).

Ao ser infectado, o computador era reiniciado automaticamente enquanto encriptava os dados. Em seguida, surgia na tela uma mensagem explicando que os dados do computador foram criptografados e que seria preciso pagar um certo valor em *bitcoins*[4] para resgatar os arquivos (KOHEN, 2017). Contudo, mesmo enviando a quantia ao endereço eletrônico indicado, os dados não eram recuperados.

---

[1] Espécie de *malware* cujo objetivo é apagar dados do computador que infecta, vide WIPER. Encyclopedia by Kapersky. Disponível em: <https://encyclopedia.kaspersky.com/glossary/wiper/>. Acesso em: 20 fev. 2022. *Malware* deriva da aglutinação da expressão "***mali**cious soft**ware***". É um *software* que ataca e prejudica o correto funcionamento de outro *software* vide BRADFIELD, J. C; KRAMER, S. A general definition of malware. **Journal in Computer Virology**, v.6, n.2, p. 105-114, mai. 2010. Disponível em: <https://link.springer.com/article/10.1007/s11416-009-0137-1#citeas>. Acesso em: 25 fev. 2021.

[2] Espécie de *malware* que, após infectar um computador, encripta os dados deste e demanda ao usuário um certo valor para desencriptá-los, vide CARTWRIGHT, A; CARTWRIGHT, E; CASTRO, J. H. To pay or not: game theoretic models of ransomware. **Journal of Cybersecurity**, Oxford, v.5, n.1, p. 1, 2019.

[3] São instruções que informam ao dispositivo como ele deve agir. Elas englobam os programas, procedimentos e rotinas do mecanismo, vide GOGONI, R. O que é software? Entenda o conceito por trás do que é software, que abrange desde sistemas operacionais a todos os apps que você usa diariamente. **Tecnoblog**. Disponível em: <https://tecnoblog.net/311647/o-que-e-software/>. Acesso em: 25 fev. 2021.

[4] Valor monetário utilizado como meio de pagamento. Também denominado de moeda virtual ou moeda encriptada, vide KÚBAT, M. Virtual Currency Bitcoin in the Scope of Money Definition and Store of Value. **Procedia Economics and Finance**, Amsterdam, v.30, p. 409-416, 2015.

O e-mail destinado a receber os *bitcoins* foi rapidamente excluído, e especialistas concluíram que o *wiper* causava danos irreversíveis ao disco rígido. Isso sugere que a operação não se destinava a obter recursos econômicos, mas a danificar permanentemente sistemas de TI de alvos específicos (CYBER-ATTACK, 2017b; HERN, 2017).

Embora não tenha sido a operação cibernética mais abrangente registrada[5], estima-se que o prejuízo em termos financeiros dela decorrente atingiu a marca de 10 bilhões de dólares (GREENBERG, 2019). Sem embargo, a operação NotPetya também acometeu boa parte da infraestrutura ucraniana, como seis hospitais, 6 companhias de energia, dois aeroportos, 22 bancos, sistemas de cartão de crédito, caixas automáticos (*ATMs*), ao menos 300 empresas (*Ibidem*) e os sistemas que monitoravam o reator nuclear em Chernobyl (GRIFFIN, 2017). Estima-se que 10% dos computadores na Ucrânia tornaram-se inutilizáveis (GREENBERG, 2019).

Além dos prejuízos materiais, a forma de realização da operação cibernética, designada *supply chain attack* (AFTER, 2021; GREENBERG, 2017), torna-o relevante. Nela, o responsável pela operação utiliza-se de fornecedores para alcançar seu alvo final no espaço cibernético, por exemplo, através de desenvolvedores e revendedores de *software* ou *hardware* (COMPUTER EMERGENCY RESPONSE TEAM (CERT)-UK[6], 2015 apud COMITÊ INTERNACIONAL DA CRUZ VERMELHA, 2019, p. 58).

Como acima explanado, o *ransomware* foi capaz de infiltrar computadores inicialmente por intermédio de uma atualização legítima oriunda de uma empresa de contabilidade, técnica que traz insegurança quanto à repetida máxima de que atualizações protegem dispositivos contra vírus (RANSOMWARE, 2021; REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE, 2020).

O Centro de Coordenação Nacional de Segurança Cibernética na Ucrânia divulgou que, à época dos fatos, não havia mecanismos de responsabilização no país para pessoas que ativa- ou passivamente cooperaram com os perpetradores do ataque cibernético (UCRÂNIA, 2017). Por outro lado, ataques cibernéticos que visam

---

[5] O ataque cibernético Wannacry, por exemplo, infectou mais de 75.000 computadores em 99 países, vide CYBER-ATTACK: Europol says it was unprecedented in scale. **BBC**, 13 mai. 2017a. Disponível em:<https://www.bbc.com/news/world-europe-39907965>. Acesso em: 22 mai. 2021.

[6] COMPUTER EMERGENCY RESPONSE TEAM (CERT)-UK. **Cyber-security risks in the supply chain**. London, 2015. Disponível em: <https://webarchive.nationalarchives.gov.uk/ukgwa/20160902161433/https:/www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf>. Acesso em: 02 fev. 2022.

abalar a infraestrutura de outros países em situações de guerra têm se tornado cada vez mais frequentes e sofisticados – a exemplo, o acesso em 2019 dos Estados Unidos ao sistema computacional que controlava lançamento de mísseis no Irã (BARNES, GIBBONS-NEFF, 2019) –, tornando os meios de guerra cibernéticos objeto de grande preocupação dentro do Direito Internacional Humanitário (COMITÊ INTERNACIONAL DA CRUZ VERMELHA, 2019, p.3).

A operação cibernética foi atribuída pelo Centro de Coordenação Nacional de Segurança Cibernética na Ucrânia à Federação Russa dentro de um contexto de guerra (UCRÂNIA, 2017). Outros países como Estados Unidos da América (2018) e Reino Unido da Grã-Bretanha e Irlanda do Norte (2018), além de especialistas na área (EXPERTS, 2017), chegaram à mesma conclusão, imputando a operação ao serviço de inteligência russo. Nesse sentido, pertinente mencionar que a operação cibernética NotPetya foi lançada um dia antes do aniversário da independência da Ucrânia (LANDER, SHANE, 2018) e que a maioria dos computadores infectados – cerca de 80% – foram desse país (WAKEFIELD, 2017).

A Rússia, por seu turno, rechaçou as acusações e declarou que a atribuição da operação cibernética ao país é desprovida de embasamento, sendo parte de uma campanha, alicerçada no ódio contra russos, promovida por alguns países ocidentais (KREMLIN, 2018; RUSSIA, 2018).

Impende destacar o contexto de crise política e social na Ucrânia quando do lançamento da operação cibernética. A doutrina, mesmo que com compreensões diversas sobre os seus motivos subjacentes, costuma citar os protestos em 2013-2014 em Maidan como o marco inicial (ou estopim) para a crise na Ucrânia (FAUNDES, 2016, p. 144; MEARSHEIMER, 2014, p. 4; TSYBULENKO, FRANCIS, 2018, p. 130).

Conforme relatado pelo Alto Comissariado das Nações Unidas para os Direitos Humanos da Organização das Nações Unidas (ONU) (2014, p. 3), os protestos populares iniciaram em 21/11/2013 no país após decisão do então Presidente Viktor Yanukovych em não assinar um acordo com a União Europeia. Como pano de fundo para as manifestações estavam insatisfações com um sistema descrito como corrupto e com um judiciário incapaz de assegurar direitos.

Ainda consoante o órgão da ONU (2014, *loc. cit*), os protestos foram retaliados com força excessiva pela polícia, em especial em Maidan - a praça de independência em Kiev, capital da Ucrânia –, culminando na votação do Parlamento Ucraniano para remoção de Yanukovych em 22/02/2014, mesmo dia em que este foi para a Rússia

(NEILD, URQUHART, 2014). Por sua vez, o presidente da Rússia, Vladimir Putin, declarou que se tratou, na verdade, de um golpe de Estado organizado pelos Estados Unidos (LONAS, 2021).

O novo governo, pró-europeu, gerou novas demonstrações na região leste da Ucrânia – notadamente nas províncias de Donesk e Luhansk – e na capital da República Autônoma da Crimeia, Simferopol, que também integrava o país (TPI - GABINETE DA PROMOTORIA, 2016, p. 35).

Em 27/02/2014, indivíduos armados sem qualquer insígnia – havendo o governo russo posteriormente admitido participação de suas forças armadas na ação – subjugaram prédios do governo em Simferopol (TPI - GABINETE DA PROMOTORIA, 2016, *loc. cit*.). Nessa toada, em 16 de março do mesmo ano, realizou-se um referendo na península da Crimeia, em que mais de 90% da população votou pela incorporação do território à Rússia (CRIMEA, 2014), considerado inválido pelo governo ucraniano (TPI - GABINETE DA PROMOTORIA, 2016, *loc. cit*.). A Rússia afirmou que agiu para proteger os cidadãos russos na Ucrânia, havendo recebido um convite pelo então Presidente Yanukovych e pelo Primeiro-Ministro da Crimeia para oferecer assistência militar, e comparou a situação da Crimeia com a secessão do Kosovo em relação à Sérvia (ALLISON, 2014, p. 1259 e 1264).

Paralelamente a isso, em abril e maio de 2014, após o governo ucraniano anunciar uma operação antiterrorismo na região leste com uso de suas forças armadas (MCCARTHY, YUHAS, 2014), a população local assumiu o controle de prédios estatais. Em 11/05/2014, as províncias de Donetsk e Luhansk também realizaram um referendo, e se declararam independentes da Ucrânia, manifestando a intenção de fazer parte da Rússia (TPI - GABINETE DA PROMOTORIA, 2016, p. 35). Há indícios de que os grupos “separatistas” locais foram ajudados financeiramente (MYKHNENKO, 2020, p. 550) e militarmente (MITROKHIN, 2015; UKRAINE, 2014) pela Rússia.

Além da operação cibernética NotPetya, a Ucrânia atribuiu à Rússia operações cibernéticas dirigidas contra a rede de energia do país em 2015 (ZETTER, 2016) e 2016 (UKRAINE, 2017), e contra um sistema regional de tratamento de água em 2018 (OSBORNE, 2018).

Conquanto não haja consenso em relação aos responsáveis pela operação cibernética NotPetya, neste artigo partir-se-á da suposição de que a operação adveio

de agentes militares russos, pois o exame jurisdicional do caso só é possível uma vez delimitada (ainda que imprecisamente) a autoria.

Ultrapassada essa observação e a breve exposição fática, passa a se analisar os pressupostos jurisdicionais para processamento do caso no Tribunal Penal Internacional (TPI).

2. REQUISITOS JURISDICIONAIS

Para que um crime específico possa ser processado pelo TPI, este deve cumprir com os requisitos e pressupostos de jurisdição[7], além dos requisitos de admissibilidade delineados nos artigos 5 a 17 do Estatuto de Roma. Todavia, presente artigo, em razão de seu recorte, não analisará o requisito de admissibilidade.

Entre os requisitos para o exercício da jurisdição encontram-se o temporal (*ratione temporis*), o territorial (*ratione loci*) ou em razão da nacionalidade (*ratione personae*), e o material (*ratione materiae*) – que o crime corresponda a um dos tipos penais presentes nos arts. 6 a 8*bis* do Estatuto. Ademais, a jurisdição só poderá ser exercida nos casos previstos nos arts. 12(3)[8] e 13[9] do supramencionado diploma

---

[7] A versão em português do Estatuto de Roma constante do Decreto nº 4.388, de 25 de Setembro de 2002 ora traduz o termo j*urisdiction* como jurisdição, ora como competência. Optei utilizar somente jurisdição como tradução de *jurisdiction* por reputar que esse conceito condiz mais com o espírito do original e a fim de tornar seu uso uniforme ao decorrer do texto.

[8] Artigo 12
Condições Prévias ao Exercício da Jurisdição
[...]
3. Se a aceitação da competência do Tribunal por um Estado que não seja Parte no presente Estatuto for necessária nos termos do parágrafo 2º, pode o referido Estado, mediante declaração depositada junto do Secretário, consentir em que o Tribunal exerça a sua competência em relação ao crime em questão. O Estado que tiver aceito a competência do Tribunal colaborará com este, sem qualquer demora ou exceção, de acordo com o disposto no Capítulo IX. In: BRASIL. Decreto nº 4.388, de 25 de Setembro de 2002. Promulga o Estatuto de Roma do Tribunal Penal Internacional. **Portal da Legislação,** Brasília, DF, 25 set. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/d4388.htm>. Acesso em: 02 fev. 2022.

[9] Artigo 13
Exercício da Jurisdição
O Tribunal poderá exercer a sua jurisdição em relação a qualquer um dos crimes a que se refere o artigo 5º, de acordo com o disposto no presente Estatuto, se:
a) Um Estado Parte denunciar ao Procurador, nos termos do artigo 14, qualquer situação em que haja indícios de ter ocorrido a prática de um ou vários desses crimes;
b) O Conselho de Segurança, agindo nos termos do Capítulo VII da Carta das Nações Unidas, denunciar ao Procurador qualquer situação em que haja indícios de ter ocorrido a prática de um ou vários desses crimes; ou
c) O Procurador tiver dado início a um inquérito sobre tal crime, nos termos do disposto no artigo 15. In: BRASIL. Decreto nº 4.388, de 25 de Setembro de 2002. Promulga o Estatuto de Roma do Tribunal Penal Internacional. **Portal da Legislação,** Brasília, DF, 25 set. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/d4388.htm>. Acesso em: 02 fev. 2022.

legal: quando a situação[10] é referida por um dos Estados Parte ao Gabinete do Promotor do TPI, quando o Conselho de Segurança encaminha a situação ao Gabinete do Promotor amparado no Capítulo VII da Carta das Nações Unidas, quando o Promotor inicia *proprio motu* uma investigação nos moldes do art. 15 do Estatuto, ou quando um Estado não Parte aceita a jurisdição do Tribunal para determinado crime por meio de depósito de declaração junto do Secretário do TPI.

Partindo-se da hipótese que a operação cibernética NotPetya amolda-se ao crime de guerra de dirigir intencionalmente ataques a bem civis – art. 8(2)(b)(ii) do Estatuto de Roma, necessário se faz verificar se o TPI possui jurisdição sobre os (a) eventos cometidos na Ucrânia (b) ao tempo da operação cibernética, 27/06/2017, (c) se a conduta ocorreu no contexto de e associada a um conflito armado internacional, e se a conduta consiste em (d) dirigir um ataque (e) a bens civis (TPI, 2013).

Para os fins deste artigo não serão perquiridos os elementos subjetivos dos Elementos dos Crimes (*Elements of Crimes*) referentes ao art. 8(2)(b)(ii) – a de que o perpetrador queria que objetos civis fossem o objeto do ataque e que o perpetrador estava ciente das circunstâncias fáticas que determinavam a existência de um conflito armado (TPI, 2013) –, vez que sua análise demanda a individualização precisa da autoria, que, a seu turno, só poderá ser obtida mediante investigação do caso.

3. JURISDIÇÃO TEMPORAL, TERRITORIAL E NACIONAL

Conquanto a Ucrânia não seja um Estado Parte do Estatuto de Roma, o país depositou junto ao Secretário do Tribunal declaração aceitando a jurisdição do órgão a partir de 20/02/2014 para investigar, processar e julgar crimes contra humanidade e crimes de guerra cometidos por oficiais da Federação Russa e líderes das organizações terroristas “DNR” e “LNR” (UCRÂNIA, 2015) cometidos em seu território.

Uma vez que a operação cibernética NotPetya ocorreu em 27/06/2017, não há maiores dificuldades em constatar que o aspecto temporal é abrangido pela

[10] Situação é a delimitação do escopo temporal, territorial (ou, em alguns casos, pessoal) dos procedimentos previstos no Estatuto de Roma que apuram se uma situação em particular deve ensejar uma investigação criminal, bem como os procedimentos da investigação propriamente dita vide TRIBUNAL PENAL INTERNACIONAL. Pre-Trial Chamber I. Situation in the Democratic Republic of the Congo. **Decision on the Applications for Participation in the Proceedings of VPRS 1, VPRS 2, VPRS 3, VPRS 5, VPRS, 5 and VPRS 6**. ICC-01/04-101-tEN-Corr. The Hague, 17 fev. 2006. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2006_01689.PDF>. Acesso em: 30 mai. 2022.

declaração. Outrossim, com a jurisdição do TPI aceita por meio de declaração oficial do país, resta atendido o disposto no art. 12(3) do Estatuto de Roma.

No que diz respeito ao requisito territorial e pessoal, segundo o artigo 12(2)(a) e 12(2)(b) do Estatuto de Roma[11], o Tribunal tem jurisdição se a conduta em questão (*conduct in question*) foi cometida no território de um Estado Parte do Estatuto (ou que depositou declaração, no caso), ou quando o acusado é nacional deste Estado.

Considerando a atribuição da operação cibernética a cidadãos russos, o critério da nacionalidade não autorizaria a persecução penal, porquanto a Rússia, em que pese ter assinado o Estatuto de Roma, nunca o ratificou, havendo retirado sua assinatura em 2016 (GRAMER, 2016).

O critério da territorialidade, por sua vez, enfatiza que o poder de jurisdição existe sobre o território onde ocorreu a conduta (quando o local é um navio ou aeronave, o Estatuto utiliza a expressão crime), apontando a doutrina que o termo foi utilizado como substituto para "ação ou omissão", não aludindo, a princípio, ao local do resultado/consequências (VAGIAS, 2011, p. 111-114) ou aos dos efeitos (SCHABAS, 2011, p. 82)[12].

Visto que somente os efeitos ou consequências do ataque cibernético aconteceram na Ucrânia, não existiria fundamento para o Tribunal exercer jurisdição. Tal óbice, contudo, pode ser contornado se a definição de "conduta" não for aplicada estritamente.

O TPI enfrentou o tema em precedentes de 2018 e 2019. Em 2018, o TPI (2018, para. 72), por meio da Câmara de Pré-Julgamento I, assinalou que há jurisdição nos termos do art. 12(2)(a) se ao menos um elemento ou parte do crime é cometido no território de um Estado Parte. Chegando a uma conclusão semelhante, a Câmara

---

[11] Artigo 12
Condições Prévias ao Exercício da Jurisdição
[...]
2. Nos casos referidos nos parágrafos a) ou c) do artigo 13, o Tribunal poderá exercer a sua jurisdição se um ou mais Estados a seguir identificados forem Partes no presente Estatuto ou aceitarem a competência do Tribunal de acordo com o disposto no parágrafo 3º:
a) Estado em cujo território tenha tido lugar a conduta em causa, ou, se o crime tiver sido cometido a bordo de um navio ou de uma aeronave, o Estado de matrícula do navio ou aeronave;
b) Estado de que seja nacional a pessoa a quem é imputado um crime. In: BRASIL. Decreto nº 4.388, de 25 de Setembro de 2002. Promulga o Estatuto de Roma do Tribunal Penal Internacional. **Portal da Legislação,** Brasília, DF, 25 set. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/d4388.htm>. Acesso em: 02 fev. 2022.

[12] *A contrario sensu* WAGNER, M. The ICC and its Jurisdiction – Myths, Misperceptions and Realities, p.485. In: PHILIPP, C. E (Ed.); VON BOGDANDY, A (Ed.); WOLFRUM, A (Ed.). **Max Planck Yearbook of United Nations Law, v. 7, 2003**. Leiden/Boston: Martinus Nijhoff Publishers, p. 409-512, 2004.

de Pré-Julgamento III declarou que o TPI poderá exercer jurisdição se ao menos parte do *actus reus*[13] – que pode englobar em certos casos a consequência do ato (TPI, 2019b, para. 50) – ocorrer em um Estado Parte (*Ibidem*, para. 61).

Como fundamentos para a primeira decisão, evocou-se que o crime ali investigado, deportação como crime contra a humanidade, implica mais de um Estado (TPI, 2018, para. 71), e que um grande número de países requerem, para estabelecer jurisdição, somente que um elemento ou parte do crime se dê em seu território (*Ibidem*, para. 66). Afora isso, a intenção dos elaboradores do Estatuto era de que o TPI possuísse jurisdição tal qual os Estados possuíam em seus sistemas jurídicos próprios. Assim, uma interpretação do referido art. 12(2)(a) que não levasse em conta esse aspecto seria incompatível com o objeto e finalidade do Estatuto de Roma (*Ibidem*, para. 69-70).

O segundo precedente foi embasado, similarmente, no fato de que os Estados Partes delegam sua jurisdição ao TPI e, não havendo eles explicitamente restringido essa delegação, presume-se que transferiram ao Tribunal a mesma jurisdição territorial que possuem no campo do Direito Internacional (TPI, 2019b, para. 60). Nesse sentido, depois de analisar o Direito de vários países, a Câmara de Pré-Julgamento III deduziu que os Estados são livres para determinar sua jurisdição territorial criminal desde que haja um link entre a conduta criminosa e seu território (*Ibidem*, para. 58).

Somado a isso, argumentou a Câmara que uma interpretação do art. 12(2)(a) que circunscrevesse a jurisdição do TPI aos crimes exclusivamente ocorridos em Estados Partes (isto é, a conduta e a consequência ocorrem em um mesmo território) vai de encontro ao princípio da boa-fé interpretativa (*Ibidem*, para. 59), porquanto não há indícios de que esta foi a intenção dos elaboradores do Estatuto. Em especial, destacou-se que entendimento contrário impediria o TPI de conhecer crimes de guerra cometidos em parte no território de um Estado não parte do Estatuto (*Ibidem*, para. 60).

Por fim, acerca dos territórios ocupados na Ucrânia (ver ponto 4.1), têm-se que o TPI não tem questionado a existência de jurisdição quando o território ocupado

[13] O termo *actus reus*, dependendo do contexto, pode incluir a conduta, as circunstâncias presentes e o resultado. Em outros, refere-se só à conduta, ou à conduta e ao resultado vide CLARK, R. S. The Mental Element in International Criminal Law: The Rome Statute of the International Criminal Court and the Elements of Offences. **Criminal Law Forum**, Boston, v.12, n. 3, nota de rodapé 10, 2001.

faz parte do TPI – independentemente da posição de Estado Parte ou não do ocupante (TSILONIS, 2019, p. 44; VAGIAS, 2011, p. 198-205).

Dessarte, caso a orientação do TPI continue a mesma, é possível afirmar que o Tribunal possui jurisdição territorial para processar o caso.

4. JURISDIÇÃO MATERIAL

4.1. CLASSIFICAÇÃO DO(S) CONFLITO(S) ARMADO(S) NO TERRITÓRIO DA UCRÂNIA

Os crimes de guerra no Estatuto de Roma são previstos em seu art. 8º, e foram em grande medida inspirados em proibições já existentes em tratados que regulam o direito nos conflitos armados (*jus in bello*) (NEWTON, 2015, p. 739-740). Dessa forma, a estrutura do referido artigo manteve a distinção costumeira do Direito Internacional Humanitário entre conflitos armados internacionais e não internacionais (COTTIER, 2016, p. 312).

De pronto, é necessário consignar que dentro de um mesmo território podem coexistir conflitos armados internacionais e não internacionais a depender de cada ator envolvido (TPI, 2012, para. 540; *idem*, 2016, para. 129). Também se faz mister ressaltar que, em razão da dificuldade em encontrar diversidade de fontes que apreciassem juridicamente o(s) conflito(s) na Ucrânia ao tempo da operação cibernética, optou-se por referenciar autoridades que analisaram a situação até 27/06/2017 – caso de Heinsch e do Relatório de 2016 do Gabinete da Promotoria do TPI – ou que, embora tenham a averiguado depois, reportam-se substancialmente a fatos ocorridos anteriormente a esta data – neste plano encontra-se Tsybulenko em 2018 e Szpak em setembro de 2017. Foi feita uma exceção ao Relatório de 2020 do Gabinete da Promotoria do TPI, porquanto pouco diferiu da análise realizada em 2016 neste ponto.

Feitas essas ressalvas, importa proceder a qualificação do(s) conflito(s) armado(s) na Ucrânia como internacional ou não internacional em 27/06/2017, tendo em vista principalmente a consequência prática de que o crime de atacar bens civis em conflitos armados internacionais (TPI, 2010, para. 33) – art. 8(2)(b)(ii) – e o crime de causar dano colateral em excesso em conflitos armados internacionais (BARTELS,

2020, p. 642) – art. 8(2)(b)(iv) – não encontram correspondente nos conflitos armados não internacionais dentro do Estatuto de Roma.

Não há uma definição específica de “conflito armado” nas Convenções de Genebra, tampouco nos Protocolos Adicionais ou no Estatuto de Roma. Dessa forma, a jurisprudência do TPI (2012, para. 533; *idem*, 2016, para. 218; *idem*, 2019a, para. 700-701) tem usado o conceito cunhado no caso *Tadić* do Tribunal Penal Internacional da Ex-Iugoslávia, o qual está assim redigido:

> [...] há um conflito armado quando é utilizada força armada entre Estados ou violência por um período extenso entre autoridades governamentais e grupos organizados armados ou por tais grupos entre si dentro de um Estado (TRIBUNAL PENAL INTERNACIONAL DA EX-IUGOSLÁVIA, Tadić, 1995, para. 70, tradução nossa)[14].

Em verdade, tal definição enunciada no caso *Tadić* condensou em um parágrafo os conceitos de conflito armado internacional e conflito armado não internacional (BARTELS, 2020, p. 602), os quais demandam diferentes requisitos.

Em linhas gerais, pode-se dizer que um conflito armado é internacional se (i) um Estado usa de força armada contra outro Estado ou território, seja mediante suas forças armadas, seja através de outros atores, inclusive privados (COTTIER, 2016, p. 313); ou (ii) quando há a ocupação parcial ou total de um território – isto é, quando o território se encontra sob a autoridade do exército inimigo (*Ibidem*, p. 314; TPI, 2012, para. 542).

Particularmente no caso em que um Estado se utiliza de outros atores não estatais para agir em seu lugar em um conflito previamente interno (intervenção indireta), o TPI (2012, para. 541; *idem*, 2019a, para. 727; *idem*, 2021, para. 2687) tem seguido o standard de “controle geral” (*overall control)* concebido no caso *Tadić* do Tribunal Penal Internacional da Ex-Iugoslávia, significativamente mais baixo (BARTELS, 2020, p. 603) do que o “controle efetivo” (*effective control)* exposto no caso *Nicaragua* da Corte Internacional de Justiça (ONU, 1986, para. 110-116).

A principal diferença entre os testes reside no grau de controle que um Estado exerce sobre o grupo adversário de outro Estado. Em que pese ambos os testes considerarem que o mero financiamento, treinamento ou equipagem de grupos não

[14] “[…] an armed conflict exists whenever there is a resort to armed force between States or protracted violence between governmental authorities and organized armed groups or between such groups within a State”.

sejam suficientes para concluir que um conflito armado tornou-se internacional, o "controle geral" requer que o Estado desempenhe um papel em organizar, coordenar ou planejar as ações militares do grupo (TRIBUNAL PENAL INTERNACIONAL DA EX-IUGOSLÁVIA, 1999, para. 131-137)[15], enquanto o controle efetivo exige que o Estado dê instruções específicas em relação às operações militares (ONU, 2007, para. 399-400).

Por sua vez, um conflito armado não internacional requer para sua caracterização que (i) haja certa intensidade; e (ii) que a parte não estatal do conflito seja um grupo armado organizado (TPI, 2019a, para. 703; *idem*, 2021, para. 2683).

O elemento intensidade estipula que deve haver um conflito armado prolongado, afastando situações de mero distúrbio interno ou atos de violência esporádicos, conforme própria indicação do art. 8(2)(f) do Estatuto de Roma, o qual também se aplica a outros artigos que cuidam de conflitos armados não internacionais (TPI, 2016, para. 133-134). Entre os fatores que sinalizam tal intensidade estão o número e duração dos confrontos, a extensão temporal e territorial dos ataques, o tipo de armas usadas, a gravidade dos ataques, e a existência de acordos de cessar fogo (TPI, 2016, para. 137; *idem*, 2019a, para. 706).

No tocante ao elemento organização, são levados em conta fatores como a existência de hierarquia interna, presença de regras e estruturas de comando, a intensidade do envolvimento militar, a capacidade do grupo de planejar e realizar operações militares coordenadas, o nível de disciplina, a capacidade do grupo de se exprimir mediante um porta-voz, entre outros (TPI, 2016, para. 134; *idem*, 2019, para. 704).

A doutrina e o Gabinete da Promotoria do TPI vislumbram dois contextos separados de conflito armado na Ucrânia: um na Crimeia e outro na sua região leste.

Quanto à situação na Crimeia, o cerne da questão se encontra na validade do referendo realizado em 16/03/2014, em que mais de 90% dos habitantes votaram a favor da região passar integrar a Rússia (CRIMEA, 2014). Isto porque, consoante a

[15] Em verdade, o Tribunal Penal da Ex-Iugoslávia, no parágrafo 137 da decisão referida, diferencia situações em que um indivíduo singular ou um grupo não organizado militarmente atua como um órgão de fato do Estado dos casos em que o controle é exercido sobre forças armadas ou milícias. Na primeira hipótese, o controle só seria aferido se houvessem instruções específicas do Estado ao grupo ou indivíduo, ou endossamento ou aprovação pública pelo Estado do ato. O teste do controle geral, por sua vez, só poderia ser utilizado na segunda situação. Todavia, não se encontraram decisões do TPI em que o ator em análise não fosse militar e, por conseguinte, a distinção em comento não foi aprofundada.

maioria dos especialistas consultados pelo Comitê Internacional da Cruz Vermelha (2012, p. 21), a ausência de consentimento do território é pressuposto para a existência de uma ocupação. Entre os motivos elencados para questionar a validade do referendo estão: sua inconstitucionalidade diante da proibição de secessão na Carta Magna ucraniana, o fato de que havia tropas russas no território quando da realização do referendo, o diminuto intervalo de 10 dias entre o chamamento para o referendo e sua votação, e a falta de clareza legal dos procedimentos tendo em vista a ausência de leis locais sobre o processo de referendo (PETERS, 2014).

Reputando-o inválido, haveria ao menos desde 18/03/2014 uma ocupação na região, visto que nesta data que a Crimeia passou a se encontrar sob a autoridade da Rússia. Assim, tratar-se-ia de um conflito armado internacional. Neste sentido é a posição da Assembleia-Geral da ONU (2019), do Gabinete da Promotoria do TPI (TPI - GABINETE DA PROMOTORIA, 2016, p. 35-36; *idem*, 2020, p. 68-69) e de parte da doutrina (HEINSCH, 2015, p. 353-354; SZPAK, 2017, p. 272-273).

Com relação à região leste da Ucrânia, o Gabinete da Promotoria do TPI ainda não assumiu uma posição definitiva sobre a (não) internacionalidade do conflito, embora tenha sugestionado em relatório de 2016 que a detenção de membros das forças militares da Rússia pela Ucrânia (e vice-versa) e acusações recíprocas de bombardeio apontavam para confronto militar direito entre as forças armadas dos dois países (TPI - GABINETE DA PROMOTORIA, 2016, p. 70-71). Ademais, declarou que examinava a hipótese de que a Rússia estaria exercendo controle geral sobre os grupos armados antigoverno nessa região (*Ibidem*, p. 36-37).

Heinsch (2015, p. 357-360) disse não haver elementos suficientes para afirmar envolvimento direto da Rússia na região leste do país, ao passo que Szpak (2017, p. 272) considerou que sim. Ambos os autores não descartaram a possibilidade do controle geral da Rússia sobre grupos separatistas pró-russos, especialmente em face de pronunciamentos oficiais de Putin (SZPAK, 2017, p. 274-275), da entrega de armas da Rússia para o leste da Ucrânia, e da anexação da Crimeia pela Rússia (Heinsch, 2015, p. 358-359). Tsybulenko e Francis (2018, p. 131-135), de outra banda, sustentam que o conflito na região, desde o início, é essencialmente entre Rússia e Ucrânia, sendo os grupos antigoverno meros colaboradores sob o controle geral das forças armadas da Rússia.

Sem embargo, na ausência de controle geral da Rússia sobre os grupos separatistas, é possível avaliar o conflito entre tais grupos e o governo da Ucrânia

como armado não internacional, uma vez que estão presentes os requisitos de organização - os grupos possuem estrutura hierárquica e realizaram operações militares coordenadas (TPI - GABINETE DA PROMOTORIA, 2016, p. 37; SZPAK, 2017, p. 274) – e de intensidade – o alto número de vítimas, o uso de armamento pesado, a duração das hostilidades e os dois acordos de cessar-fogo de Minsk apontam neste sentido (HEINSCH, 2015, p. 355; TPI - GABINETE DA PROMOTORIA, 2016, p. 37; TPI - GABINETE DA PROMOTORIA, 2020, p. 69).

Urge por último relembrar que pode ocorrer simultaneamente um conflito armado internacional entre os dois países e um armado não internacional entre a Ucrânia e os grupos separatistas (TPI, 2012, para. 565).

Em suma, a natureza do conflito armado na Ucrânia, em especial em sua região leste, é extremamente controvertido, e sua qualificação demandará extensa análise fática e jurídica por parte do TPI.

4.2. NEXO ENTRE A CONDUTA E O(S) CONFLITO(S) ARMADO(S)

O requisito de que a conduta criminosa esteja associada ao conflito armado é interpretado pela jurisprudência do TPI (2016, para. 142-143; *idem*, 2019a, para. 731-732; *idem*, 2021, para. 2683) como a necessidade de que tal conflito tenha tido um papel substancial na decisão, habilidade ou maneira de cometer o crime. Não se exige, todavia, que este tenha sido o motivo fundamental do cometimento, podendo a conduta ocorrer em lugares e momentos distintos daquele das hostilidades. Nesta perspectiva, são levados em contas fatores como (i) o status do perpetrador e da vítima (e se exerceram algum papel nas hostilidades), (ii) se o ato em questão se presta a atingir o objetivo final de uma campanha militar, e (iii) se o crime foi cometido como parte/no contexto das funções oficiais do perpetrador.

No que toca à relação da operação cibernética NotPetya com os conflitos armados na Ucrânia, não há informações suficientes a respeito do terceiro fator mencionado, posto que necessária a individualização da autoria. Contudo, torna-se relevante o fato de que, como referido anteriormente, a operação foi lançada no dia anterior ao comemorativo da Independência da Ucrânia e teve como porta de entrada um sistema contábil largamente utilizado por civis no país, havendo os governos estadunidense e do Reino Unido aduzido que a operação destinou-se a desestabilizar

o governo e as Finanças da Ucrânia (ESTADOS UNIDOS DA AMÉRICA, 2018; REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE, 2018).

Isso posto, a verificação do link entre a operação cibernética em comento e o(s) conflito(s) na Ucrânia exigirá maior obtenção de informações pelo Gabinete da Promotoria do TPI, vez que a pesquisa empreendida não logrou encontrar elucidação robusta sobre as razões do lançamento da operação.

4.3. EXISTÊNCIA DE UM ATAQUE

O primeiro elemento específico do crime 8(2)(b)(ii) é que tenha ocorrido um ataque. Não há conceito de ataque no Estatuto de Roma, tampouco no documento titulado Elementos dos Crimes. Não obstante não haja precedentes específicos sobre o crime em questão no TPI, ao decidir sobre outros crimes de guerra o órgão adotou a definição contida no art. 49(1)[16] do Protocolo Adicional às Convenções de Genebra de 1949 (I Protocolo), esclarecendo que se trata de um ato de violência contra o adversário, seja ofensivo ou defensivo (TPI, 2008, para. 266; *idem*, 2010, para. 65; *idem*, 2014, para. 45).

Tradicionalmente a violência exigida para configurar um ataque corresponderia à liberação de força cinética. No entanto, a doutrina consultada propala o entendimento de que não é possível reter-se estritamente à noção de força cinética sob pena de excluir agentes químicos, biológicos ou radiológicos das limitações do Direito Internacional Humanitário. Assim, compreendem que a violência diz respeito aos efeitos ou consequências do ato (DÖRMANN, 2016, p. 356; DROEGE, 2012, p. 557). Outrossim, a Corte Internacional de Justiça, ao abordar o uso das armas nucleares, enfatizou que os princípios do Direito Internacional Humanitário aplicam-se a todas as formas de combate e a todo tipo de armas, inclusive as do futuro (ONU, 1996, para. 78). Nesse diapasão, uma operação

---

[16] ARTIGO 49
Definição de Ataques e Campo de Aplicação
1. Entende-se por "ataques" os atos de violência contra o adversário, sejam ofensivos ou defensivos. In: BRASIL. DECRETO Nº 849, DE 25 DE JUNHO DE 1993. Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados. **Portal da Legislação**, Brasília, DF, 25 jun. 1993. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0849.htm>. Acesso em: 02 fev. 2022.

cibernética poderia constituir um ataque se os seus efeitos fossem análogos aos da força cinética (DROEGE, 2012, p. 546; SCHMITT, VIHUL, 2017, p. 415).

Entretanto, esse posicionamento teórico não é isento de discussões. Não há consenso sobre o que representa um efeito análogo ao da força cinética para os fins do Direito Internacional Humanitário.

Especialistas consultados na elaboração do Tallinn Manual 2.0 consideraram que uma operação cibernética atinge o *standard* de ataque quando há razoável expectativa de que esta cause lesões a pessoas (incluindo grave sofrimento mental ou desenvolvimento de doenças), morte, e destruição, ou dano a objetos (SCHMITT, VIHUL, 2017, p. 415-417), ao passo que o Comitê Internacional da Cruz Vermelha (2020, p. 481-492) afirma que a noção de ataque também abarca operações cibernéticas que resultem em perda de funcionalidade da infraestrutura cibernética. Dörmann (2004, p. 4) esposa a segunda posição, reportando-se à definição de objetivo militar contida no art. 52(2) do I Protocolo, a qual coloca a neutralização de um objeto no mesmo patamar que sua destruição ou captura. Ademais, debate-se se danos reversíveis e perdas de funcionalidade temporárias são suficientes para qualificar a operação cibernética como um ataque (AMBOS, 2015, p. 123; DROEGE, 2012, p. 559).

Pertinente ainda mencionar que o termo objetos (*objects*), de acordo com o Comentário dos Protocolos Adicionais das Convenções de Genebra, deve ser interpretado como algo visível e tangível/palpável (COMITÊ INTERNACIONAL DA CRUZ VERMELHA, 1987, p. 634)[17], resultando na conclusão de que destruição ou dano aos dados (*data*) presentes na infraestrutura cibernética atingida não configuram um ataque (SCHMITT, VIHUL, 2017, p. 413, 437).

Sem embargo, o TPI (2008, para. 270; *idem*, 2019a, para. 904) possui precedentes relativos aos crime de guerra de dirigir ataques intencionalmente a civis em conflitos internacionais – art. 8(2)(b)(i) – e não internacionais – art.8(2)(e)(i) – nos quais declarou que não há necessidade de ocorrer qualquer tipo de dano para a configuração do delito, consumando-se com o mero lançamento do “ataque”. Em outro precedente sobre o mesmo crime, o TPI (2014, para. 46) reproduziu o posicionamento

[17] Para diferentes entendimentos cf. DÖRMANN, K; GISEL, L; RODENHÄUSER T. Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. **International Review of the Red Cross**, v. 102, n. 913, Digital technologies and war, p. 318-319, 2020.

de que a violência constituinte de um ataque manifesta-se em suas consequências, especialmente quando são desejadas ou esperadas lesões, morte, danos ou destruição.

Desse modo, considerando que as consequências da operação cibernética NotPetya foram a perda da funcionalidade da infraestrutura cibernética, interrupção de serviços, prejuízos financeiros e perda de dados, a sua caracterização como um ataque dependerá largamente da tomada de posição do TPI a uma das concepções do termo ataque em que os efeitos físicos são (quase) imperceptíveis.

4.4. STATUS DOS OBJETOS ATACADOS

A proibição de atacar objetos civis, além de regra constante do art. 52 do I Protocolo, é reputada como norma costumeira no Direito Internacional advinda do princípio da distinção (COMITÊ INTERNACIONAL DA CRUZ VERMELHA 2009, p. 25), o qual é considerado um princípio cardinal do Direito Internacional Humanitário (ONU, 1996, para. 78).

O Estatuto de Roma fornece o conceito de objetos civis no seu art. 8(2)(b)(ii), definindo-o como objetos que não são objetivos militares – claramente uma remissão aos dispositivos do I Protocolo (AMBOS, 2014, p. 150). O art. 52(2) do I Protocolo determina que objetivos militares são

> aqueles objetos que por sua natureza, localização, finalidade ou utilização contribuam eficazmente para a ação militar ou cuja destruição total ou parcial, captura ou neutralização, ofereça nas circunstâncias do caso presente uma vantagem militar definida (BRASIL, 1993).

Embora o Decreto nº 849/93 utilize a conjunção “ou” em seu texto entre “ação militar” e “cuja destruição”, a versão autoritativa em inglês prevê em seu lugar o termo “*and*”, denotando que são requisitos cumulativos (AMBOS, 2014, p. 150; DÖRMANN, 2016, p. 363).

O primeiro requisito estabelece que deve haver um estreito nexo causal entre o alvo e a ação militar por pelo menos um dos quatro critérios (natureza, localização, finalidade ou utilização) (DROEGE, 2012, p. 559). Objetos que contribuem para a ação militar por sua natureza tipicamente abarcam os usados diretamente pelas forças

armadas, tais como equipamentos militares e infraestrutura militar. O critério da localização inclui objetos que estão em uma área geográfica de particular importância militar (DÖRMANN, 2016, p. 363). Já os critérios da finalidade e do uso cuidam de objetos a princípio civis que serão ou são utilizados para fins militares (SCHMITT, VIHUL, 2017, p. 438-440). Nesse sentido, deve haver indicadores concretos de que o objeto será no futuro empregado para tais fins, não bastando mera suspeita de que será utilizado (DÖRMANN, 2016, p. 363).

Por sua vez, o segundo requisito demanda o prospecto de uma vantagem militar definida advinda do ataque, como o enfraquecimento das forças militares adversárias (KLAMBERG, 2017, p. 80). O adjetivo militar indica que vantagens políticas, econômicas ou psicológicas – como atemorizar a população civil (AMBOS, 2014, p. 151; DINSTEIN, 2004, p. 116), não entram no escopo de um objetivo militar (SCHMITT, VIHUL, 2017, p. 442), ao passo que o termo “definida” exclui vantagens indeterminadas ou hipotéticas (COMITÊ INTERNACIONAL DA CRUZ VERMELHA, 1987, p. 636), devendo a vantagem ser concreta e perceptível (DÖRMANN, 2016, p. 363). A vantagem pode ser aferida em relação ao ataque isoladamente ou à operação como um todo (AMBOS, 2014, p. 191).

Apresenta-se de especial relevância para o tema os chamados “*dual-use objects*”, os quais são objetos usados tanto por civis quanto militares. Em realidade, não há a possibilidade de um objeto ser simultaneamente civil ou militar (SCHMITT, VIHUL, 2017, p. 445), devendo os critérios acima expostos ser aplicados caso a caso (COMITÊ INTERNACIONAL DA CRUZ VERMELHA, 2009, p. 32). Em vista disso, a doutrina aponta a complexidade cyberespaço: em última instância, praticamente toda a infraestrutura cibernética é usada por civis e militares (DROEGE, 2012, p. 559), e dificilmente será possível especificar por qual parte da rede as transmissões de cunho militar serão remetidas (SCHMITT, VIHUL, 2017, p. 446). Destarte, o princípio da distinção no cyberespaço teria sua aplicação extremamente limitada (AMBOS, 2015, p. 132).

Examinando a operação NotPetya, têm-se que alguns dos objetos atingidos podem ser considerados alvos que contribuem para a ação militar pelo seu uso. É o caso da infraestrutura cibernética afetada, conforme acima explanado, e o da rede de energia (DINSTEIN, 2004, p. 116). Por outro lado, vários objetos atingidos são

claramente de uso civil[18], como os pertences a empresas privadas afetadas, e não há evidências de que qualquer dos alvos - mesmo os objetos que em princípio contribuem para a ação militar – tenha oferecido qualquer vantagem militar definitiva (BILLER, SCHMITT, 2017).

Dessarte, é razoável considerar, *prima facie*, que os objetos eram objetos civis. Não obstante, na hipótese do Tribunal julgar que os requisitos do duplo teste foram cumpridos e que, portanto, o ataque foi dirigido a um ou mais objetivos militares, há ainda a possibilidade de que a ação seja contida no tipo do art. 8(2)(b)(iv), *in verbis*:

> iv) Lançar intencionalmente um ataque, sabendo que o mesmo causará perdas acidentais de vidas humanas ou ferimentos na população civil, danos em bens de caráter civil ou prejuízos extensos, duradouros e graves no meio ambiente que se revelem claramente excessivos em relação à vantagem militar global concreta e direta que se previa;

De acordo com precedentes do TPI (2008, para. 274; *idem*, 2007, para. 41), o crime do art. 8(2)(b)(iv) se aplica a situações em que um ataque é lançado com vistas a atingir especificamente objetivos militares, mas com a ciência de que irão ou poderão sobrevir danos colaterais, como lesões acidentais de civis.

Entretanto, o artigo não criminaliza a ocorrência de danos incidentais em si mesmo (AMBOS, 2015, p. 134). Referido tipo penal remonta ao princípio da proporcionalidade do Direito Internacional Humanitário (AMBOS, 2014, p. 176) - cuja expressão se encontra no art. 51(5)(b)[19] do I Protocolo (COMITÊ INTERNACIONAL DA CRUZ VERMELHA, 2009, p. 46) -, assim, o ato amolda-se ao art. 8(2)(b)(iv) na

---

[18] Em tese, o fato da operação cibernética NotPetya ter afligido hospitais pode – se demonstrado que foi intencional – caracterizar o crime de guerra presente no art. 8(2)(b)(iii) do Estatuto de Roma. Contudo, a subsunção do fato a esse tipo penal não será analisada no presente artigo em razão de seu recorte.

[19] ARTIGO 51
Proteção da população civil
[...]
5. Considerar-se-ão indiscriminados, entre outros, os seguintes tipos de ataque:
[...]
b) os ataques quando se pode prever que causarão incidentalmente mortos e ferimentos entre a população civil, ou danos a bens de caráter civil, ou ambas as coisas, e que seriam excessivos em relação a vantagem militar concreta e diretamente prevista. In: BRASIL. DECRETO Nº 849, DE 25 DE JUNHO DE 1993. Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados. **Portal da Legislação**, Brasília, DF, 25 jun. 1993. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0849.htm>. Acesso em: 02 fev. 2022.

medida em que os danos colaterais sejam classificados como claramente excessivos em comparação com a vantagem militar como um todo esperada.

Ataques indiscriminados podem, em certas circunstâncias, violar o princípio da proporcionalidade (TRIBUNAL PENAL INTERNACIONAL DA EX-IUGOSLÁVIA, 2003, para. 58), sendo, nesses casos, passíveis de enquadramento no art. 8(2)(b)(iv) (AMBOS, 2014, p. 177). Como exemplo de ataques indiscriminados, citam-se os que atingem indistintamente objetivos militares e objetos civis em razão do emprego de método ou meios de combate cujos efeitos não conseguem ser controlados da maneira como o Direito Internacional Humanitário prescreve[20], e aqueles em que vários objetivos militares precisos e claramente separados são tratados como um único objetivo militar (SCHMITT, VIHUL, 2017, p. 469).

De acordo com especialistas na área, o(s) autor(es) da operação cibernética tinha(m) acesso ao número de identificação de cada entidade cadastrada com o governo da Ucrânia para fins tributários, e, teoricamente, poderia(m) ter lançado a operação cibernética contra alvos precisos, e não contra todos os que utilizavam o *software* MeDoc (GREENBERG, 2019).

Dessarte, conclui-se que, a depender da apreciação fática, a operação cibernética pode ajustar-se ao tipo penal do art. 8(2)(b)(ii) do Estatuto de Roma, um ataque contra objetos civis, ou ao art. 8(2)(b)(iv) do mesmo diploma legal, um ataque indiscriminado desproporcional. Destaca-se que a caracterização da operação cibernética como um ataque indiscriminado, porém proporcional, encontra-se em um vácuo legislativo dentro do TPI, nada obstante ser proibido na seara do Direito Internacional Humanitário (COMITÊ INTERNACIONAL DA CRUZ VERMELHA, 2009, p. 37-35).

---

[20] ARTIGO 51
Proteção da população civil
[...]
4. São proibidos os ataques indiscriminados. São ataques indiscriminados:
[...]
c) aqueles que empregam métodos ou meios de combate cujos efeitos não seja possível limitar conforme o exigido pelo presente Protocolo;
[...]
e que em conseqüência, em qualquer de tais casos possam atingir indistintamente a objetivos militares e as pessoas civis ou a bens de caráter civil. In: BRASIL. DECRETO Nº 849, DE 25 DE JUNHO DE 1993. Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados. **Portal da Legislação**, Brasília, DF, 25 jun. 1993. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0849.htm>. Acesso em: 02 fev. 2022.

Por fim, salutar mencionar que o Gabinete da Promotoria declarou no Relatório de Investigações Preliminares de 2020 que há substrato razoável para acreditar que, a partir de 30 de abril de 2014 em diante, na região leste da Ucrânia, ocorreram os crimes de guerra de intencionalmente dirigir ataques a bens civis – art. 8(2)(b)(ii) ou art. 8(2)(e)(i) do Estatuto de Roma, dependendo da classificação do conflito armado. Ademais, se caracterizado um conflito armado internacional, haveria também substrato razoável para acreditar que houve lançamento intencional de um ataque, o qual causou danos a bens de caráter civil e foi claramente excessivo em relação à vantagem militar global concreta e direta prevista – art. 8(2)(b)(iv) (TPI - GABINETE DA PROMOTORIA, 2020, p. 70-71). Tais declarações, todavia, não deixam claro quais dos fatos apurados mereceram tal tipificação, não havendo qualquer alusão a operações cibernéticas ao longo do relatório.

5. CONCLUSÃO

O artigo em tela objetivou averiguar se o TPI possui jurisdição sobre a operação cibernética denominada NotPetya partindo da suposição de que o fato ocorrido se enquadra no tipo penal do art. 8(2)(b)(ii) do Estatuto de Roma. Primeiramente relatou-se a ocorrência da operação cibernética em comento, com ênfase nos seus efeitos no território ucraniano e sua ligação com os conflitos ali existentes, passando em seguida a expor sucintamente a conjuntura em que a operação foi lançada.

No ponto seguinte exploraram-se os requisitos jurisdicionais para que o caso fosse apreciado pelo TPI, sem se enfrentar a questão da admissibilidade. Verificou-se que a Ucrânia depositou uma declaração junto ao órgão em 20/02/2014, aceitando a jurisdição do tribunal para os crimes de guerra e contra a humanidade ocorridos no território desde esta data, satisfazendo, portanto, o requisito da jurisdição temporal e o contido no art. 12(3) do Estatuto de Roma. Observou-se também que há diferentes interpretações do termo “conduta” presente no art. 12(2)(a) do Estatuto de Roma, mas que a jurisdição territorial no caso concreto pode ser exercida se forem levadas em conta decisões recentes do TPI, as quais adotam o entendimento de que o vocábulo “conduta” ali referido contempla as consequências do crime.

Subsequentemente, decompôs-se a apreciação do requisito material segundo os elementos objetivos do crime do art. 8(2)(b)(ii). No tocante à existência de um

conflito armado internacional, constatou-se que havia, na época dos fatos, dois polos de conflito na Ucrânia – um na região autônoma da Crimeia e outro no leste do país - e que há divergência na doutrina sobre o envolvimento russo no segundo polo do conflito, não havendo o Gabinete da Promotoria do TPI se posicionado terminantemente sobre sua caracterização. Quanto ao nexo entre a conduta criminosa e o conflito armado, as informações fáticas colhidas não permitiram assertar sua existência, necessitando maiores investigações. Concluiu-se, ainda, que a qualificação da operação NotPetya como um ataque em matéria de Direito Internacional Humanitário é controvertida, tendo em vista as diversas correntes existentes sobre o que constitui um “efeito análogo ao da força cinética”, em especial na esfera cibernética. Por derradeiro, compreendeu-se que os objetos atingidos pela operação em comento podem ser categorizados como civis, uma vez que a operação lançada não aparentou oferecer qualquer vantagem militar definida. Alternativamente, não se tratando de objetos civis, entreviu-se a possibilidade da conduta incorrer no tipo do art. 8(2)(b)(iv) do Estatuto de Roma.

Em 2020, o Gabinete da Promotoria do TPI encerrou o exame preliminar na situação da Ucrânia, assinalando que o próximo passo seria requerer à Câmara de Pré-Julgamento autorização para iniciar uma investigação (STATEMENT, 2020). Todavia, somente após a invasão da Rússia à Ucrânia em 2022 (UKRAINE, 2022) foi que o Promotor atual do TPI declarou que solicitaria a uma das Câmaras de Pré-Julgamento do Tribunal a abertura da investigação no país (STATEMENT, 2022a). Com as atenções do mundo redobradas para a região, 39 Estados Partes referiram a situação da Ucrânia ao Gabinete da Promotoria, permitindo que a investigação fosse iniciada em 02/03/2022, sem necessidade de passar pelo órgão judicial (STATEMENT, 2022b).

Conclusivamente, conquanto o acirramento dos conflitos ali presentes tenha viabilizado uma tramitação e processamento mais rápidos da situação no Tribunal, o fato da operação cibernética NotPetya não ter causado danos diretamente ao seres humanos (em contraposição a outros crimes de guerra tradicionais a serem apurados), a incerteza jurídica em torno de crimes de guerra cometidos pela via cibernética, e a discussão teórica em torno do termo “conduta” para aferir a jurisdição territorial são fatores que podem levar o Gabinete da Promotoria a não priorizar o caso perante o Tribunal.

REFERÊNCIAS

AFTER hack, officials draw attention to supply chain threats: The U.S. government is working to draw attention to supply chain vulnerabilities. **Independent**, 01 abr. 2021. Disponível em: <https://www.independent.co.uk/news/after-hack-officials-draw-attention-to-supply-chain-threats-washington-notpetya-twitter-orlando-harvard-university-b1825619.html>. Acesso em: 22 mai. 2021.

ALLISON, R. Russian 'deniable' intervention in Ukraine: how and why Russia broke the rules. **International Affairs**, Oxford-Malden, v. 90, n. 6, p. 1255-1297, 2014.

AMBOS, K. International criminal responsibility in cyberspace. In: BUCHAN, R (Ed.).; TSAGOURIAS, N. (Ed). **Research Handbook on International Law and Cyberspace**. Cheltenham: Edward Elgar Publishing Limited, p. 118-143, 2015.

AMBOS, K. **Treatise on International Criminal Law Volume II: The Crimes and Sentencing**. Oxford: Oxford University Press, 2014.

BARTELS, R. The Classification of Armed Conflicts by International Criminal Courts and Tribunals. **International Criminal Law Review**, The Hague, v. 20, n. 4, p. 595–668, 2020.

BARNES, J. E.; GIBBONS-NEFF, T. U.S. Carried Out Cyberattacks on Iran. **The New York Times**, 22 jun. 2019. Disponível em: <https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html>. Acesso em: 22 set. 2020.

BILLER, J.; SCHMITT M; **The NotPetya Cyber Operation as a Case Study of International Law**, 11 jul. 2017. EJIL: Talk!. Disponível em:<https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/>. Acesso em: 02 fev. 2022.

BRASIL. Decreto nº 4.388, de 25 de Setembro de 2002. Promulga o Estatuto de Roma do Tribunal Penal Internacional. **Portal da Legislação,** Brasília, DF, 25 set. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/d4388.htm>. Acesso em: 02 fev. 2022.

BRASIL. Decreto nº 849, de 25 de junho de 1993. Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados. **Portal da Legislação,** Brasília, DF, 25 jun. 1993. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0849.htm>. Acesso em: 02 fev. 2022.

BRADFIELD, J. C; KRAMER, S. A general definition of malware. **Journal in Computer Virology**, v. 6, n. 2, p. 105-114, mai. 2010. Disponível em: <https://link.springer.com/article/10.1007/s11416-009-0137-1#citeas>. Acesso em: 25 fev. 2021.

CARTWRIGHT, A; CARTWRIGHT, E; CASTRO, J. H. To pay or not: game theoretic models of ransomware. **Journal of Cybersecurity**, Oxford, v. 5, n. 1, p. 1-12, 2019.

CLARK, R. S. The Mental Element in International Criminal Law: The Rome Statute of the International Criminal Court and the Elements of Offences. **Criminal Law Forum**, Boston, v. 12, n. 3, p. 291-334, 2001.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. Doswald-Beck, L; Henckaerts, J. **Customary International Humanitarian Law: volume I, rules**. Cambridge: Cambridge University Press, 2009.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. Ferraro, T. (Ed.). **Expert Meeting**: Occupation and other forms of Administration of Foreign Territory. Geneva, 2012. Relatório. Disponível em: <https://www.icrc.org/en/doc/assets/files/publications/icrc-002-4094.pdf>. Acesso em: 19 fev. 2022.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. Gisel, L; Olejnik, L. **The Potential Human Cost of Cyber Operations**. ICRC Expert Meeting 14-16 November 2018 – Geneva. Geneva, 2019. Disponível em: <https://www.icrc.org/en/document/potential-human-cost-cyber-operations>. Acesso em: 23 mai. 2021.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. International humanitarian law and cyber operations during armed conflicts: ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019. **International Review of the Red Cross**, v. 102, n. 913, Digital technologies and war, p. 481-492, 2020.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. Sandoz, Y (Ed.); Swinarski, C. (Ed.); Zimmermann, B. (Ed.). **Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949**. Geneva: Martinus Nijhoff Publishers, 1987.

COMPUTER EMERGENCY RESPONSE TEAM (CERT)-UK. **Cyber-security risks in the supply chain**. London, 2015. Disponível em: <https://webarchive.nationalarchives.gov.uk/ukgwa/20160902161433/https:/www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf>. Acesso em: 02 fev. 2022 apud COMITÊ INTERNACIONAL DA CRUZ VERMELHA. GISEL, L; OLEJNIK, L. **The Potential Human Cost of Cyber Operations**. ICRC Expert Meeting 14-16 November 2018 – Geneva. Geneva, 2019. Disponível em: <https://www.icrc.org/en/document/potential-human-cost-cyber-operations>. Acesso em: 23 mai. 2021.

COTTIER, M. Article 8. Part I: Introduction/ General Remarks. In: AMBOS, K (Ed.); TRIFFTERER, O (Ed.). **The Rome Statute of the International Criminal Court**: A Commentary. Munich/Oxford/Baden-Baden: C.H. Beck/Hart/Nomos, p. 304-321, 2016.

CRIMEA referendum: Voters 'back Russia union'. **BBC**, 16 mar. 2014. Disponível em: <https://www.bbc.com/news/world-europe-26606097>. Acesso em: 19 fev. 2022.

CYBER-ATTACK: Europol says it was unprecedented in scale. **BBC**, 13 mai. 2017a. Disponível em:<https://www.bbc.com/news/world-europe-39907965>. Acesso em: 22 mai. 2021.

CYBER-ATTACK was about data and not money, say experts. **BBC**, 29 jun. 2017b. Disponível em: <https://www.bbc.com/news/technology-40442578>. Acesso em: 22 mai. 2021.

DINSTEIN, Y. **The Conduct of Hostilities under the Law of International Armed Conflict**. Cambridge: Cambridge University Press, 2004.

DÖRMANN, K. Article 8 para. 2: Meaning of 'war crimes In: AMBOS, K (Ed.); TRIFFTERER, O (Ed.). **The Rome Statute of the International Criminal Court: A Commentary**. Munich/Oxford/Baden-Baden: C.H. Beck/Hart/Nomos, 2016.

DÖRMANN, K. **The Applicability of the Additional Protocols to Computer Network Attacks**: An ICRC Viewpoint. In: International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17-19 nov. 2004, Stockholm. Disponível em: <https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf>. Acesso em: 31 jan. 2021.

DÖRMANN, K; GISEL, L; RODENHÄUSER T. Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. **International Review of the Red Cross**, v. 102, n. 913, Digital technologies and war, p. 287-334, 2020.

DROEGE, CORDULA. Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. **International Review of the Red Cross**, v. 94, n. 886, p. 533-578, 2012.

ESTADOS UNIDOS DA AMÉRICA. Secretaria de Imprensa. **Statement from the Press Secretary - foreign policy**. 15 fev. 2018. Disponível em: <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>. Acesso em: 25 set. 2020.

EXPERTS Say NotPetya Cyberattack Came From Russia. **PYMNTS**, 07 jul. 2017. Disponível em: <https://www.pymnts.com/news/security-and-risk/2017/cybersecurity-experts-say-notpetya-cyberattack-came-from-russia/#:~:text=Experts%20Say%20NotPetya%20Cyberattack%20Came%20From%20Russia&text=Experts%20are%20saying%20that%20the,the%20originator%20of%20the%20attack> . Acesso em: 23 set. 2020.

FAUNDES, C. An Analysis of the Crisis in Ukraine, and its Three Conflicts (21 of November 2013, through 23 of May 2014). **Revista de Relaciones Internacionales, Estrategia y Seguridad**, Bogotá, v. 11, n. 2, p. 137-159, jul./dez. 2016.

FAYI, S. Y. A. What Petya/NotPetya Ransomware Is and What Its Remediations Are. In: LATIFI, S (Ed.). **Information Technology - New Generations 15th International Conference on Information Technology Series: Advances in Intelligent Systems and Computing**. Berlin: Springer, p. 93-100, 2018.

GOGONI, R. O que é software? Entenda o conceito por trás do que é software, que abrange desde sistemas operacionais a todos os apps que você usa diariamente. **Tecnoblog**. Disponível em: <https://tecnoblog.net/311647/o-que-e-software/>. Acesso em: 25 fev. 2021.

GRAMER, R. Why Russia Just Withdrew from the ICC: The ICC has had a rough year, and Russia just made things worse. **Foreign Policy**, 16 nov. 2016. Disponível em: <https://foreignpolicy.com/2016/11/16/why-russia-just-withdrew-from-icc-putin-treaty-ukraine-law/>. Acesso em: 22 set. 2020.

GREENBERG, A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. **Wired**, 22 ago. 2018. Disponível em: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>. Acesso em: 23 set. 2020.

GREENBERG, A. Software Has a Serious Supply-Chain Security Problem: Hackers have targeted software's supply chain in three high profile attacks discovered over the summer. **Wired**, 09 out. 2017. Disponível em:<https://www.wired.com/story/ccleaner-malware-supply-chain-software-security/>. Acesso em: 22 mai. 2021.

GREENBERG, A. **Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers**. New York: Doubleday, 2019. *E-book*.

GRIFFIN, A. 'Petya' cyber attack: Chernobyl's radiation monitoring system hit by worldwide hack: Monitoring is now being performed manually, Ukrainian authorities said". **Independent**, 27 jun. 2017. Disponível em: <https://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html>. Acesso em: 22 mai. 2021.

HEINSCH, Robert. Conflict Classification in Ukraine: The Return of the "Proxy War"? **International Law Studies**, Newport, Rhode Island, v. 91, n. 323, p. 321-360, 2015.

HERN, A. Ransomware attack 'not designed to make money', researchers claim: Digital security researchers say malware attack that spread from Ukraine appeared to be focused on damaging IT systems. **The Guardian**, 28 jun. 2017. Disponível em: <https://www.theguardian.com/technology/2017/jun/28/notpetya-ransomware-attack-ukraine-russia>. Acesso em: 23 set. 2020.

KLAMBERG, M (Ed.). **Commentary on the Law of the International Criminal Court**. Brussels: Torkel Opsahl Academic EPublisher, 2017.

KOHEN, I. WannaCry, Now NotPetya: How to Protect Yourself from Cyber Outbreaks. **IT Security Central - Teramind Blog**, 06 jul. 2017. Disponível em:

<https://itsecuritycentral.teramind.co/2017/07/06/wannacry-now-notpeyta-how-to-protect-yourself-from-cyber-outbreaks/>. Acesso em: 23 set. 2020.

KREMLIN slams ‘Russophobic’ allegations that pin NotPetya cyber attack on Russia: Moscow repudiates accusations of being involved in the NotPetya cyber attack that had struck Ukraine in June 2017. **Russian news agency TASS**, 15 fev. 2018. Disponível em:<https://tass.com/politics/990154?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com>. Acesso em: 26 abr. 2022.

KÚBAT, M. Virtual Currency Bitcoin in the Scope of Money Definition and Store of Value. **Procedia Economics and Finance**, Amsterdam, v. 30, p. 409-416, 2015.

LANDER, M.; SHANE S. U.S. Condemns Russia for Cyberattack, Showing Split in Stance on Putin. **The New York Times**, 15 fev. 2018. Disponível em: <https://www.nytimes.com/2018/02/15/us/politics/russia-cyberattack.html>. Acesso em: 23 set. 2020.

LONAS, L. Putin accuses US of organizing 2014 Ukraine coup. **The Hill**, 22 jun. 2021. Disponível em:<https://thehill.com/policy/international/russia/559557-putin-accuses-us-of-organizing-2014-ukraine-coup/>. Acesso em 28 abr. 2022.

MCCARTHY, T; YUHAS, A. Ukraine crisis: Kiev launches 'anti-terror operation' in east – live updates. **The Guardian**, 15 abr. 2014. Disponível em: <https://www.theguardian.com/world/2014/apr/15/ukraine-military-forces-russia-live-blog?view=desktop#block-534d962be4b07648e2d90f44> . Acesso em: 23 fev. 2022.

MEARSHEIMER, J.J. Why the Ukraine Crisis Is the West’s Fault: The Liberal Delusions That Provoked Putin. **Foreign Affairs**, New York, p. 1-12, v. 93, n. 5, set./out. 2014.

MICROSOFT DEFENDER ATP RESEARCH TEAM. New ransomware, old techniques: Petya adds worm capabilities. **Microsoft**, 27 jun. 2017. Disponível em: <https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc>. Acesso em: 23 set. 2020.

MITROKHIN, N. Infiltration, Instruction, Invasion: Russia’s War in the Donbass. **Journal of Soviet and Post-Soviet Politics and Society**, Stuttgart, v. 1. n. 1, p. 229-249, 2015.

MYKHNENKO, V. Causes and Consequences of the War in Eastern Ukraine: An Economic Geography Perspective, **Europe-Asia Studies**, London, v. 72, n. 4, p. 528-560, 2020.

NEILD, N; URQUHART, C. Ukraine: Tymoshenko freed as president denounces 'coup' - 22 February as it happened. **The Guardian**, 23 fev. 2014. Disponível em:<https://www.theguardian.com/world/2014/feb/22/ukraine-crisis-uncertainty-after-yanukovych-signs-deal-live-updates>. Acesso em: 23 fev. 2022.

NEWTON, A. M. Charging War Crimes: Policy and Prognosis from a Military Perspective. In: STAHN, C (Ed.). **The Law and the Practice of the International Criminal Court**. Oxford: Oxford University Press, p. 732-760, 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Alto Comissariado das Nações Unidas para os Direitos Humanos. **Report of the United Nations High Commissioner for Human Rights on the situation of human rights in Ukraine**. A/HRC/27/75. New York, 19 set. 2014. Disponível em: <https://digitallibrary.un.org/record/780616>. Acesso em: 22 fev. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Assembleia-Geral. **Resolution adopted by the General Assembly on 17 December 2018 [without reference to a Main Committee (A/73/L.47 and A/73/L.47/Add.1)] Problem of the militarization of the Autonomous Republic of Crimea and the city of Sevastopol, Ukraine, as well as parts of the Black Sea and the Sea of Azov**. A/RES/73/194. New York, 23 jan. 2019. Disponível em: <https://digitallibrary.un.org/record/1661591?ln=en>. Acesso em: 25 set. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Corte Internacional de Justiça. Case concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide, Bosnia and Herzegovina v. Serbia and Montenegro. **Judgment of 26 February 2007**. The Hague, 26 fev. 2007. Disponível em: <https://www.icj-cij.org/public/files/case-related/91/091-20070226-JUD-01-00-EN.pdf>. Acesso em: 25 set. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Corte Internacional de Justiça. Legality of the threat or use of nuclear weapons. **Advisory Opinion of 8 July 1996**. The Hague, 08 jul. 1996. Disponível em: <https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf>. Acesso em: 25 set. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Corte Internacional de Justiça. Military and Paramilitary Activities in and against Nicaragua, Nicaragua v. United States of America. **Merits, Judgment**. The Hague, 27 jun. 1986. Disponível em: <https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf>. Acesso em: 25 set. 2020.

OSBORNE, C. Ukraine blocks VPNFilter attack against core country water system: Russia has been blamed for the cyberattack. **ZDNet**, 13. jul. 2018. Disponível em: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>. Acesso em: 26 fev. 2022.

PETERS, A**.** Sense and Nonsense of Territorial Referendums in Ukraine, and Why the 16 March Referendum in Crimea Does Not Justify Crimea's Alteration of Territorial Status under International Law. **EJIL: Talk!**, 16 abr. 2014. Disponível em: <https://www.ejiltalk.org/sense-and-nonsense-of-territorial-referendums-in-ukraine-and-why-the-16-march-referendum-in-crimea-does-not-justify-crimeas-alteration-of-territorial-status-under-international-law/>. Acesso em: 20 fev. 2022.

RANSOMWARE. **Microsoft**, 14 abr. 2021. Disponível em: https://docs.microsoft.com/pt-br/windows/security/threat-

protection/intelligence/ransomware-malware>. Acesso em: 23 mai. 2021; REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE. National Cyber Security Centre. **Mitigating malware and ransomware attacks**. 13 fev. 2020. Disponível em:<https://www.ncsc.gov.uk/pdfs/guidance/mitigating-malware-and-ransomware-attacks.pdf>. Acesso em: 23 mai. 2021.

REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE. Centro Nacional de Segurança Cibernética. **Russian military 'almost certainly' responsible for destructive 2017 cyber attack**. 14 fev. 2018. Disponível em: <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack>. Acesso em: 25 set. 2020.

RUSSIA denies British allegations that Moscow was behind cyber-attack. **Reuters**, 15 fev. 2018. Disponível em: <https://www.reuters.com/article/us-britain-russia-cyber-kremlin-idUSKCN1FZ102>. Acesso em: 26 abr. 2022.

SCHABAS, W. **An Introduction to the International Criminal Court**. Cambridge: Cambridge University Press, 2011.

SCHMITT, N. M. (Ed.); VIHUL, L. (Ed.). **Tallinn Manual 2.0 on the International Law applicable to Cyber Operations: prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence**. Cambridge: Cambridge University Press, 2017.

STATEMENT of the Prosecutor, Fatou Bensouda, on the conclusion of the preliminary examination in the situation in Ukraine. **ICC-CPI**, 11 dez. 2020. Disponível em: <https://www.icc-cpi.int/Pages/item.aspx?name=201211-otp-statement-ukraine> . Acesso em: 21 mar. 2022.

STATEMENT of ICC Prosecutor, Karim A.A. Khan QC, on the Situation in Ukraine: "I have decided to proceed with opening an investigation." **ICC-CPI**, 28 fev. 2022a. Disponível em: <https://www.icc-cpi.int/Pages/item.aspx?name=20220228-prosecutor-statement-ukraine>. Acesso em: 21 mar. 2022.

STATEMENT of ICC Prosecutor, Karim A.A. Khan QC, on the Situation in Ukraine: Receipt of Referrals from 39 States Parties and the Opening of an Investigation. **ICC-CPI**, 02 mar. 2022b. Disponível em: <https://www.icc-cpi.int/Pages/item.aspx?name=2022-prosecutor-statement-referrals-ukraine> Acesso em: 21 mar. 2022.

SZPAK, A. Legal classification of the armed conflict in Ukraine in light of international humanitarian law. **Hungarian Journal of Legal Studies**, Budapest, v. 58, n. 3, p. 261–280, 2017.

TRIBUNAL PENAL INTERNACIONAL DA EX-IUGOSLÁVIA. Appeals Chamber. Prosecutor v. Duško Tadić. **Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction**. IT-94-1-A. The Hague, 02 out. 1995. Disponível em: <https://www.icty.org/x/cases/tadic/acdec/en/51002.htm>. Acesso em: 25 set. 2020.

TRIBUNAL PENAL INTERNACIONAL DA EX-IUGOSLÁVIA. Appeals Chamber. Prosecutor v. Duško Tadić. **Judgement**. IT-94-1-A. The Hague, 15 jul. 1999. Disponível em: <https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf>. Acesso em: 25 set. 2020.

TRIBUNAL PENAL INTERNACIONAL DA EX-IUGOSLÁVIA. Trial Chamber. Prosecutor v. Stanislav Galić. **Judgement and Opinion**. IT-98-29-T. The Hague, 05 dez. 2003. Disponível em: <https://www.icty.org/x/cases/galic/tjug/en/gal-tj031205e.pdf>. Acesso em: 02 fev. 2022.

TRIBUNAL PENAL INTERNACIONAL. Elements of Crimes. The Hague, 2013. Disponível em: <https://www.icc-cpi.int/resource-library/Documents/ElementsOfCrimesEng.pdf>. Acesso em: 25 set. 2020.

TRIBUNAL PENAL INTERNACIONAL - GABINETE DA PROMOTORIA. **Report on Preliminary Examination Activities: 2016.** 14 nov. 2016. Disponível em: <https://www.icc-cpi.int/iccdocs/otp/161114-otp-rep-PE_ENG.pdf>. Acesso em: 25 set. 2020.

TRIBUNAL PENAL INTERNACIONAL - GABINETE DA PROMOTORIA. **Report on Preliminary Examination Activities: 2020.** 14 dez. 2020. Disponível em: <https://www.icc-cpi.int/itemsDocuments/2020-PE/2020-pe-report-eng.pdf>. Acesso em: 18 fev. 2022.

TRIBUNAL PENAL INTERNACIONAL. Pre-Trial Chamber I. Situation in the Democratic Republic of the Congo. **Decision on the Applications for Participation in the Proceedings of VPRS 1, VPRS 2, VPRS 3, VPRS 5, VPRS, 5 and VPRS 6**. ICC-01/04-101-tEN-Corr. The Hague, 17 fev. 2006. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2006_01689.PDF>. Acesso em: 30 mai. 2022.

TRIBUNAL PENAL INTERNACIONAL. Pre-Trial Chamber I. Request under Regulation 46(3) of the Regulations of the Court. **Decision on the "Prosecution's Request for a Ruling on Jurisdiction under Article 19(3) of the Statute"**. ICC-01/19-27. The Hague, 06 set. 2018. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2018_04203.PDF>. Acesso em: 25 set. 2020.

TRIBUNAL PENAL INTERNACIONAL. Pre-Trial Chamber I. Situation in the Darfur, Sudan in the case of The Prosecutor v. Bahar Idriss Abu Garda. **Decision on the confirmation of charges**. ICC-02/05-02/09-243-Red. The Hague, 08 fev. 2010. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2010_00753.PDF>. Acesso em: 25 set 2020.

TRIBUNAL PENAL INTERNACIONAL. Pre-Trial Chamber I. Situation in the Democratic Republic of the Congo in the case of The Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui. **Decision on the confirmation of charges**. ICC-01/04-01/07-717. The Hague, 30 set. 2008. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2008_05172.PDF>. Acesso em: 25 set. 2020.

TRIBUNAL PENAL INTERNACIONAL. Pre-Trial Chamber I. Situation in the Democratic Republic of the Congo in the case of The Prosecutor v. Germain

Katanga. **Decision on the evidence and information provided by the Prosecution for the issuance of a warrant of arrest for Germain Katanga**. ICC-01/04-01/07-4. The Hague, 06 jul. 2007. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2007_03883.PDF>. Acesso em: 25 set. 2020.

TRIBUNAL PENAL INTERNACIONAL. Pre-Trial Chamber II. Situation in the Democratic Republic of the Congo in the case of The Prosecutor v. Bosco Ntaganda. **Decision Pursuant to Article 61(7)(a) and (b) of the Rome Statute on the Charges of the Prosecutor Against Bosco Ntaganda**. ICC-01/04-02/06-309. The Hague, 09 jun. 2014. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2014_04750.PDF>. Acesso em: 25 set. 2020.

TRIBUNAL PENAL INTERNACIONAL. Pre-Trial Chamber III. Situation in the People's Republic of Bangladesh/Republic of the Union of Myanmar. **Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the People's Republic of Bangladesh/Republic of the Union of Myanmar**. ICC-01/19-27. The Hague, 14 nov. 2019b. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2019_06955.PDF>. Acesso em: 25 set. 2020.

TRIBUNAL PENAL INTERNACIONAL. Trial Chamber I. Situation in the Democratic Republic of the Congo in the case of The Prosecutor v. Thomas Lubanga Dyilo. **Judgment pursuant to Article 74 of the Statute**. ICC-01/04-01/06-2842. The Hague, 14 mar. 2012. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2012_03942.PDF>. Acesso em: 25 set. 2020.

TRIBUNAL PENAL INTERNACIONAL. Trial Chamber III. Situation in the Central African Republic in the case of The Prosecutor v. Jean Pierre Bemba Gombo. **Judgment pursuant to Article 74 of the Statute**. ICC-01/05-01/08-3343. The Hague, 21 mar. 2016. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2016_02238.PDF>. Acesso em: 30 jan. 2021.

TRIBUNAL PENAL INTERNACIONAL. Trial Chamber IV. Situation in the Democratic Republic of the Congo in the case of The Prosecutor v. Bosco Ntaganda. **Judgment**. ICC-01/04-02/06-2359. The Hague, 08 jul. 2019a. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2019_03568.PDF>. Acesso em: 30 jan. 2021.

TRIBUNAL PENAL INTERNACIONAL. Trial Chamber IX. Situation in Uganda in the case of The Prosecutor v. Dominic Ongwen. **Trial Judgment**. ICC-02/04-01/15-1762-Red. The Hague, 04 fev. 2021. Disponível em: <https://www.icc-cpi.int/CourtRecords/CR2021_01026.PDF>. Acesso em: 30 jan. 2021.

TSILONIS, V. **The Jurisdiction of the International Criminal Court**. Springer: Cham, 2019. *E-book*.

TSYBULENKO, E; FRANCIS J. A. Separatists or Russian Troops and Local Collaborators? Russian Aggression in Ukraine: The Problem of Definitions. In: TSYBULENKO, E. (Ed.); SAYAPIN, S. (Ed). **The Use of Force against Ukraine and International Law: Jus Ad Bellum, Jus In Bello, Jus Post Bellum**. T.M.C. ASSER PRESS: The Hague, p. 123-144, 2018.

UCRÂNIA. Conselho Nacional de Segurança da Ucrânia. **Oleksandr Turchynov: One of the mechanisms for spreading a dangerous computer virus was a system for updating the accounting software**. Kiev, 29 jun. 2017. Disponível em: <https://web.archive.org/web/20180909085046/http://www.rnbo.gov.ua:80/en/news/2821.html>. Acesso em: 22 mai. 2021.

UCRÂNIA. Ministério das Relações Exteriores da Ucrânia. **Resolution of the Verkhovna Rada of Ukraine: on the Declaration of the Verkhovna Rada of Ukraine "On the recognition over crimes agains humanity and war crimes committed by senior officials of the Russian Federation and leaders of terrorists organizations "DNR" and "LNR", which led to extremely grave consequences and mass murder of Ukranian nationals"**. 08 set. 2015. Disponível em: <https://www.icc-cpi.int/iccdocs/other/Ukraine_Art_12-3_declaration_08092015.pdf>. Acesso em: 22 set. 2020.

UKRAINE crisis: Key players in eastern unrest. BBC, 28 ago. 2014. Disponível em: <https://www.bbc.com/news/world-latin-america-27211501>. Acesso em: 23 fev. 2022.

UKRAINE power cut 'was cyber-attack'. **BBC**, 11 jan. 2017. Disponível em: <https://www.bbc.com/news/technology-38573074>. Acesso em: 19 fev. 2022.

UKRAINE conflict: What we know about the invasion. **BBC**, 24 fev. 2022. Disponível em: <https://www.bbc.com/news/world-europe-60504334>. Acesso em: 21 mar. 2022.

VAGIAS, M. **The Territorial Jurisdiction of the International Criminal Court**: certain constested issues. 264 f. Thesis (PH.D). – Leiden University, Amsterdam, 2011.

WAGNER, M. The ICC and its Jurisdiction – Myths, Misperceptions and Realities. In: PHILIPP, C. E (Ed.); VON BOGDANDY, A (Ed.); WOLFRUM, A (Ed.). **Max Planck Yearbook of United Nations Law, v. 7, 2003**. Leiden/Boston: Martinus Nijhoff Publishers, p. 409-512, 2004.

WAKEFIELD, J. Taxsoftware blamed for cyberattack spread. **BBC**, 28 jun. 2017. Disponível em: <https://www.bbc.com/news/technology-40428967>. Acesso em: 22 mai. 2021.

ZETTER, K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid: The hack on Ukraine's power grid was a first-of-its-kind attack that sets an ominous precedent for the security of power grids everywhere. **Wired**, 03 mar. 2016. Disponível em: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>. Acesso em: 26 fev. 2022.