

RENATO FERREIRA JÁCOMO DOS SANTOS
STAELL DOS SANTOS STEIN

**CONSIDERAÇÕES SOBRE O FINANCIAMENTO AO TERRORISMO POR MEIO
DE CRIPTOMOEDAS E SEUS IMPACTOS PARA A SEGURANÇA E DEFESA
NACIONAIS**

Trabalho de Conclusão de Curso apresentado à
Escola Superior de Defesa, como exigência
parcial para obtenção do título de Especialista
em Altos Estudos em Defesa.

Orientador: Prof. Dr. Ivan Carlos S. de Oliveira
– Cel (EB) R1.

Brasília
2022

Este trabalho, nos termos da legislação que resguarda os direitos autorais, é considerado propriedade da Escola Superior de Defesa (ESD). É permitida a transcrição parcial de textos do trabalho, ou mencioná-los, para comentários e citações, desde que sem propósitos comerciais e que seja feita a referência bibliográfica completa. Os conceitos expressos neste trabalho são de responsabilidade dos autores e não expressam qualquer orientação institucional da ESD.



RENATO FERREIRA JACOMO DOS SANTOS

Autor



STAELL DOS SANTOS STEIN

Autora

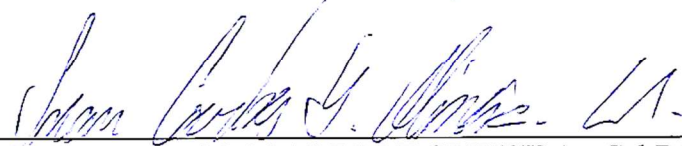
**RENATO FERREIRA JÁCOMO DOS SANTOS
STAELL DOS SANTOS STEIN**

**CONSIDERAÇÕES SOBRE O FINANCIAMENTO AO TERRORISMO POR
MEIO DE CRIPTOMOEDAS E SEUS IMPACTOS PARA A SEGURANÇA E
DEFESA NACIONAIS**

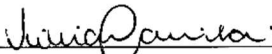
Trabalho de Conclusão de Curso
apresentado à Escola Superior de Defesa,
como exigência parcial para obtenção do
título de Especialista em Altos Estudos
em Defesa.

Trabalho de Conclusão de Curso **APROVADO:**

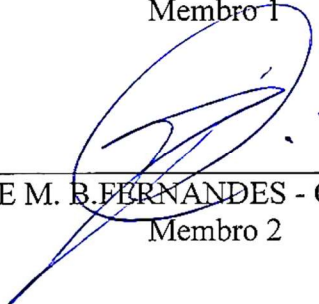
Brasília, DF, 19 de outubro de 2022



IVAN CARLOS SOARES DE OLIVEIRA - Cel R1 EB (ESD)
Orientador



VIVIANE MACHADO CAMINHA – Profa. Dra. (ESD)
Membro 1



RAFAEL DE M. B. FERNANDES - Cel R1 EB (EsIMEx)
Membro 2

Considerações sobre o uso de criptomoedas no financiamento ao terrorismo e seus impactos para a Segurança e Defesa nacionais

Renato Ferreira Jácomo dos Santos^{1a}
Staell dos Santos Stein^{2a}

RESUMO

O ataque de 11 de setembro de 2001, nos Estados Unidos da América, acarretou no desenvolvimento de novas estratégias para prevenção e combate ao terrorismo, conjugando investigações mais invasivas e esforços militares, com destaque para Forças de Operações Especiais. Com o fortalecimento dos mecanismos internacionais de repressão do financiamento ao terrorismo, as criptomoedas surgiram como alternativa para atividades ilícitas, por existir uma grande dificuldade em identificar e rastrear as transações. Criptomoedas são ativos virtuais, protegidos por criptografia, cujas operações são executadas e armazenadas numa rede de computadores. No Brasil, a Polícia Federal é responsável pelo enfrentamento do terrorismo e seu financiamento, podendo contar com o apoio do Comando de Defesa Cibernética na repressão a crimes cibernéticos. O objetivo geral deste artigo é estudar as razões pelas quais criptomoedas podem ser utilizadas como fonte de financiamento ao terrorismo, no contexto da Segurança Nacional. A metodologia desenvolvida foi a pesquisa exploratória. A conclusão aponta para a necessidade de contínua e incremental integração entre órgãos civis de Segurança e Forças Armadas, notadamente os engajados na atividade de Inteligência e no setor cibernético, tanto no âmbito internacional como no nacional. No contexto da Defesa Nacional identificam-se repercussões do tema para o estudo da Guerra Híbrida e das táticas de “Zona Cinza”.

Palavras-chave: Terrorismo; *Blockchain*; *Ransomware*; Guerra Híbrida.

Considerations about the use of cryptocurrency in terrorism financing and its impacts on National Security and Defense

ABSTRACT

The September 11th, 2001 attack in the United States of America led to the development of new strategies to prevent and combat terrorism, combining more invasive investigations and military efforts, highlighting Special Operations Forces. With the strengthening of international mechanisms to counter terrorism financing, cryptocurrency has emerged as an alternative for illicit activities, as there is great difficulty in identifying and tracking transactions. Cryptocurrencies are virtual assets, protected by cryptography, whose operations are performed and stored on a computer network. In Brazil, the Federal Police is responsible for fighting terrorism and its financing, and can count on the support of the Cyber Defense Command in the repression of cybercrimes. The general objective of this article is to study the reasons why cryptocurrencies can be used as a source of terrorism financing, in the context of National Security. The methodology developed was exploratory research. The conclusion points to the need for continuous and incremental integration between civil Security agencies and the Armed Forces, notably those engaged in the Intelligence activity and in the Cyber sector, both internationally and nationally. In the context of National Defense, repercussions of the theme are identified for the study of Hybrid Warfare and “Grey Zone” tactics.

Keywords: *Terrorism; Blockchain; Ransomware; Hybrid Warfare.*

¹ Capitão de Mar e Guerra da Marinha do Brasil, servindo no Estado-Maior Conjunto das Forças Armadas.

² Gerente do Banco do Brasil de Prevenção e Combate à Lavagem de Dinheiro, Financiamento ao Terrorismo e à Corrupção.

^a Trabalho de Conclusão do Curso de Altos Estudos em Defesa (CAED) da Escola Superior de Defesa (ESD), 2022.

1 INTRODUÇÃO

Com o fortalecimento dos mecanismos internacionais de repressão à lavagem de dinheiro, as criptomoedas surgiram como alternativa de financiamento de atividades ilícitas por parte de elementos nelas engajados, dentre os quais se destacam os grupos terroristas. As associações do uso de criptomoedas com o terrorismo são objeto de interesse para a Atividade de Inteligência em nível Estratégico e, por conseguinte, da Defesa Nacional.

Os volumes movimentados com criptomoedas estão cada vez mais elevados, e se nota a migração de movimentações financeiras ilícitas, que antes eram realizadas por doleiros, para esse segmento, devido à maior segurança que esse canal proporcionaria com a eliminação de intermediários no processo, além de tornar mais complexa a identificação das origens e dos destinos dos fluxos financeiros. Considerando que as organizações criminosas transnacionais estão utilizando dessa tipologia para fortalecer suas estruturas e formas de agir, percebem-se impactos dessa dinâmica para a Segurança Nacional.

Há uma grande necessidade de compreender o uso de criptomoedas por grupos terroristas, dada a dificuldade de identificar e rastrear o dinheiro e quem o movimenta. O uso de dinheiro por grupos terroristas pode ocorrer em três momentos: recebimento, gerenciamento e gastos. Todos esses momentos representam grandes desafios para tais grupos, especialmente no uso das criptomoedas. A escolha de qual criptomoeda será utilizada pela organização terrorista depende da tecnologia e de suas propriedades, como o anonimato e a possibilidade de proceder a transações de grandes somas, segurança, aceitação, usabilidade e confiabilidade. Por usabilidade se entende como uma facilitação com que o utente transaciona e gerencia seu próprio dinheiro.

O sistema financeiro tradicional, por sua vez, é desafiado a rever seus processos de forma a acompanhar esta inovação, o que diz respeito ao campo do Desenvolvimento Nacional.

Assim, com a abordagem do trinômio Segurança, Defesa e Desenvolvimento, justifica-se a pertinência do tema como Trabalho de Conclusão do Curso de Altos Estudos em Defesa.

O objetivo geral do presente artigo é estudar as razões pelas quais criptomoedas podem ser utilizadas como fonte de financiamento ao terrorismo, relacionando seus atributos e formas de operacionalização, os principais problemas e dificuldades enfrentados, decorrentes desse uso, no contexto da Segurança Nacional, e suas implicações para a Defesa Nacional.

O fenômeno do terrorismo será abordado de maneira sintética, limitando o escopo ao seu financiamento, sob as perspectivas internacional e nacional.

Igualmente em razão da limitação de escopo do trabalho, não serão realizadas considerações sobre o uso de criptomoedas no contexto de conflitos armados e suas modalidades de autofinanciamento.

Como objetivos específicos são elencados: identificar de que forma as criptomoedas favorecem ou se relacionam com o provimento de necessidades advindas de atividades terroristas; estudar possíveis alternativas para mitigar o uso das criptomoedas no financiamento ao terrorismo, no âmbito da cooperação interagências; e identificar como o envolvimento das Forças Armadas nesta temática poderia contribuir para o fortalecimento da Defesa Nacional.

Ao final, procurar-se-á responder à seguinte pergunta de pesquisa: “Como os organismos internacionais e o Brasil têm se preparado para enfrentar o uso de criptomoedas como meio de financiamento ao terrorismo nos campos de Segurança e Defesa Nacionais, e quais são as principais vulnerabilidades do País frente ao tema?”.

A metodologia desenvolvida foi a pesquisa exploratória, utilizando-se revisões bibliográficas e pesquisas documentais, apoiadas nas fontes disponibilizadas pelos docentes do Curso de Altos Estudos em Defesa (CAED) nas disciplinas: Segurança, Desenvolvimento e Defesa; Estudos Estratégicos; Direito Aplicado à Defesa; Geopolítica; Relações Internacionais e Defesa Nacional, bem como fontes disponíveis nas respectivas instituições dos autores (Ministério da Defesa e Banco do Brasil).

2 TERRORISMO E SEU FINANCIAMENTO

O terrorismo é um crime reconhecido internacionalmente (UNITED NATIONS, 1994, p. 4), conquanto se esteja longe do consenso quanto à sua definição. “Até os presentes dias observamos a impossibilidade de uma conceituação consensual e pacífica do fenômeno e da imprevisibilidade terrorista, fator que desafia a elaboração de estratégias preventivas e repressivas a atos terroristas” (MATOS *apud* CHUY, 2018, p. 69).

Haja vista a plêiade de publicações científicas e cursos acadêmicos que tratam especificamente da compreensão desse fenômeno, por limitação de escopo este artigo contemplará, como referencial teórico, apenas a definição legalmente estabelecida no Brasil, que será apresentada adiante.

Historicamente, o desenvolvimento de um arcabouço estratégico para a sua prevenção e combate, a nível mundial, acelerou-se a partir de 11 de setembro de 2001 (TEIDER, 2021, p. 31), data em que ocorreu, nos Estados Unidos da América (EUA), um evento terrorista de magnitude jamais vista anteriormente: o ataque coordenado aos edifícios gêmeos do *World*

Trade Center, na cidade de New York, e ao edifício do Pentágono (Secretaria de Defesa), em Washington D.C.³, juntamente com a queda de um quarto avião sequestrado em área rural da Pennsylvania, redundando na morte de aproximadamente três mil pessoas (HOFFMAN, 2002, p. 303-304). “Os dezenove terroristas que atacaram as Torres Gêmeas (...) tinham contas bancárias e receberam várias transferências internacionais” (VAN BUGGENHOUT, 2021, p. 53) que viabilizaram a ação.

As novas estratégias para prevenção e combate ao terrorismo a partir de então desenvolvidas, sob a liderança dos EUA, procuraram aliar esforços militares — na declarada Guerra Global ao Terror⁴ — ao alargamento da amplitude investigativa sobre indivíduos, organizações e atividades, visados como alvos, em paralelo ao fomento de coalizões internacionais. Surge então a expressão “Combate do Financiamento ao Terrorismo” (CFT)⁵ como o ramo de atividades com o propósito de neutralizar ou mitigar o financiamento ao terrorismo por quaisquer meios (TEIDER, 2021, 32).

Sobre o crime de financiamento ao terrorismo, Van Buggenhout (2021, p. 53) comenta que:

Ocorre quando alguém, direta ou indiretamente, ilegal e deliberadamente, fornecer ou reunir fundos com a intenção de utilizá-los, ou tendo conhecimento de que serão utilizados, total ou parcialmente, na prática de um ato que constitua terrorismo, bastando-se a tentativa. (...)

Os sujeitos ativo e passivo podem ser quaisquer pessoas que buscam financiar a prática de atos de terrorismo. Apesar de as organizações terroristas terem o costume de escolher certos alvos, tais como embaixadas, autoridades governamentais, instalações militares, além de grupos étnicos e religiosos, para a configuração do crime o agente pode agir de forma solitária, sem vinculação a alguma organização terrorista.

Em geral, os grupos terroristas necessitam de financiamento para pagamento de transporte, alojamento e alimentação daqueles que executam os ataques. Esses custos são relativamente baixos e, por isso, de difícil rastreamento. Entretanto, os maiores gastos são com armas, munições e outros artefatos voltados a espalhar o terror. Por isso, o terrorismo evoluiu e se adapta a cada dificuldade imposta pelas autoridades. Além de novas fontes de recursos, os terroristas inovam-se para utilizarem aquelas menos vulneráveis à interceptação. É indubitável que a possibilidade de os grupos terroristas contarem com a movimentação bancária tradicional foi reduzida significativamente.

³ *District of Columbia*.

⁴ *Global War on Terror (GWOT)* (WILLIAMS; OKON; OBASA, 2018, p. 1).

⁵ Do original em inglês “*Combating the Financing of Terrorism*” ou “*Counter-Financing of Terrorism*”.

Assim, o financiamento de grupos terroristas por meio de transferências diretas já não é mais a forma usual, porquanto atualmente representa alto risco para o doador, tanto financeiro quanto legal. Em razão disso, os sistemas não-convencionais de transferência de dinheiro passaram a ser visados pelas autoridades. Por exemplo, supremacistas brancos foram identificados “industrializando” suas campanhas de captação de recursos financeiros por meio da monetização de conteúdo de ódio em mídias sociais e solicitação de doações por meio de criptomoedas (INSTITUTE FOR ECONOMICS & PEACE, 2022, p. 74). Neste particular, as criptomoedas passaram a ser adotadas pelos grupos terroristas como contramedida às ações governamentais antiterror. Para os financiadores, a transferência de valores em criptomoedas para esses grupos tem de ser suficientemente robusta, segura e anônima (DION-SCHWARZ; MANHEIM; JOHNSTON, 2021, p. 9).

2.1 NO BRASIL

No Brasil, o terrorismo é elencado pela Política Nacional de Inteligência como “uma ameaça à paz e à segurança dos Estados” (BRASIL, 2016b, p. 6). Contudo, a tipificação deste crime esteve pendente entre a promulgação da Constituição Federal de 1988 e a da Lei nº13.260, de 16 de março de 2016⁶, que o definiu, em seu artigo 2º, como:

Prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.

§ 1º São atos de terrorismo:

I – usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa;

II – (VETADO);

III - (VETADO);

IV - sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino

⁶ Segundo diversos autores, a tramitação e aprovação da lei se deu a partir de pressões do Grupo de Ação Financeira (GAFI), crescentes a partir de 2015 e que incluíram ameaças de exclusão do Brasil do Grupo, “com consequências econômicas e mercadológicas negativas perante a comunidade internacional” (TEIDER, 2021, p. 65).

e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento;
V - atentar contra a vida ou a integridade física de pessoa (BRASIL, 2016a, p. 1).

Além dos atos supracitados, a lei brasileira criminaliza também, em seu artigo 6º, o respectivo financiamento:

Receber, prover, oferecer, obter, guardar, manter em depósito, solicitar, investir, de qualquer modo, direta ou indiretamente, recursos, ativos, bens, direitos, valores ou serviços de qualquer natureza, para o planejamento, a preparação ou a execução dos crimes previstos nesta Lei:

Pena - reclusão, de quinze a trinta anos.

Parágrafo único. Incorre na mesma pena quem oferecer ou receber, obtiver, guardar, mantiver em depósito, solicitar, investir ou de qualquer modo contribuir para a obtenção de ativo, bem ou recurso financeiro, com a finalidade de financiar, total ou parcialmente, pessoa, grupo de pessoas, associação, entidade, organização criminosa que tenha como atividade principal ou secundária, mesmo em caráter eventual, a prática dos crimes previstos nesta Lei (BRASIL, 2016a, p. 1-2).

Resta evidente que no Brasil a repressão ao terrorismo é assunto de Segurança Pública (gestão político-administrativa), com atuação específica da Polícia Federal, conforme o artigo 11 da lei em comento:

Para todos os efeitos legais, considera-se que os crimes previstos nesta Lei são praticados contra o interesse da União, cabendo à Polícia Federal a investigação criminal, em sede de inquérito policial, e à Justiça Federal o seu processamento e julgamento, nos termos do inciso IV do art. 109 da Constituição Federal (BRASIL, 2016a, p. 2).

De maneira coerente, no âmbito do governo federal o Ministério da Justiça e Segurança Pública, ao qual se subordina a Polícia Federal, detém a primazia da coordenação das medidas para o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados.

3 A INOVAÇÃO DAS CRIPTOMOEDAS

A principal função de uma moeda é ser meio de troca aceito por uma comunidade econômica, tendo como funções econômicas, ser: i) meio de troca, ii) medida de valor (unidade de conta), iii) reserva de valor, iv) instrumento liberatório de obrigações; v) padrão de pagamentos diferidos; e vi) instrumento de poder (LOPES; ROSSETI, 2002, p. 18).

Na década de 1990, alguns matemáticos e cientistas da computação começaram a pensar em realizar transações sem necessidade de intermediação financeira. Naquela época, tal ideia era considerada disruptiva, pois o mercado já estava muito habituado a contar com um banco para “garantir” que o dinheiro “existia” e que estava guardado em algum cofre.

Era necessário um sistema de pagamento eletrônico baseado em garantia de criptografia, que permitisse quaisquer duas partes dispostas a transacionar diretamente uma com a outra, sem a necessidade de uma terceira. Essas ideias foram tomando corpo e em 2008 foi criada a primeira criptomoeda, o Bitcoin, que possibilitou que transações pudessem ocorrer de uma pessoa para outra, de forma *on line* (BURNISKE; TATAR, 2019, p. 34).

Satoshi Nakamoto⁷ descreveu o Bitcoin como um sistema de pagamento eletrônico baseado em garantia de criptografia, o que permite quaisquer duas partes dispostas a transacionar diretamente uma com a outra. A utilização de redes de computadores P2P (“*peer to peer*”, ou “ponto a ponto”) garante as operações sem a necessidade de uma terceira pessoa e as salva cronologicamente, trazendo maiores garantias (NAKAMOTO, 2008, p. 1).

Genericamente, uma criptomoeda pode ser considerada um tipo de dinheiro, como outras moedas com as quais convivemos, mas ela não é emitida por nenhum governo (como o Real, o Dólar, ou o Euro, por exemplo). Esses ativos surgiram com a intenção de permitir que indivíduos ou empresas efetuem pagamentos ou transferências financeiras eletrônicas diretamente a outros indivíduos ou empresas, sem a necessidade da intermediação de uma instituição financeira. Tal propósito serviria, inclusive, para pagamentos ou transferências internacionais.

Segundo o Fundo Monetário Internacional (FMI), as criptomoedas são representações digitais de valor, o qual decorre da confiança depositada nas suas regras de funcionamento e na cadeia de participantes (HE *et al.*, 2016). Não são emitidas por Banco Central, de forma que não se confundem com o padrão monetário nacional, de curso forçado, ou com o padrão de qualquer outra autoridade monetária. Além disso, não se confundem com a moeda eletrônica prevista na legislação, que se caracteriza como recursos em Reais mantidos em meio eletrônico, em bancos e outras instituições, que permitem ao usuário realizar pagamentos e transferências.

⁷ À época da elaboração deste artigo desconhecia-se a real identidade por trás do pseudônimo “Satoshi Nakamoto”, inventor (ou inventores) do Bitcoin (DUCRÉE, 2022).

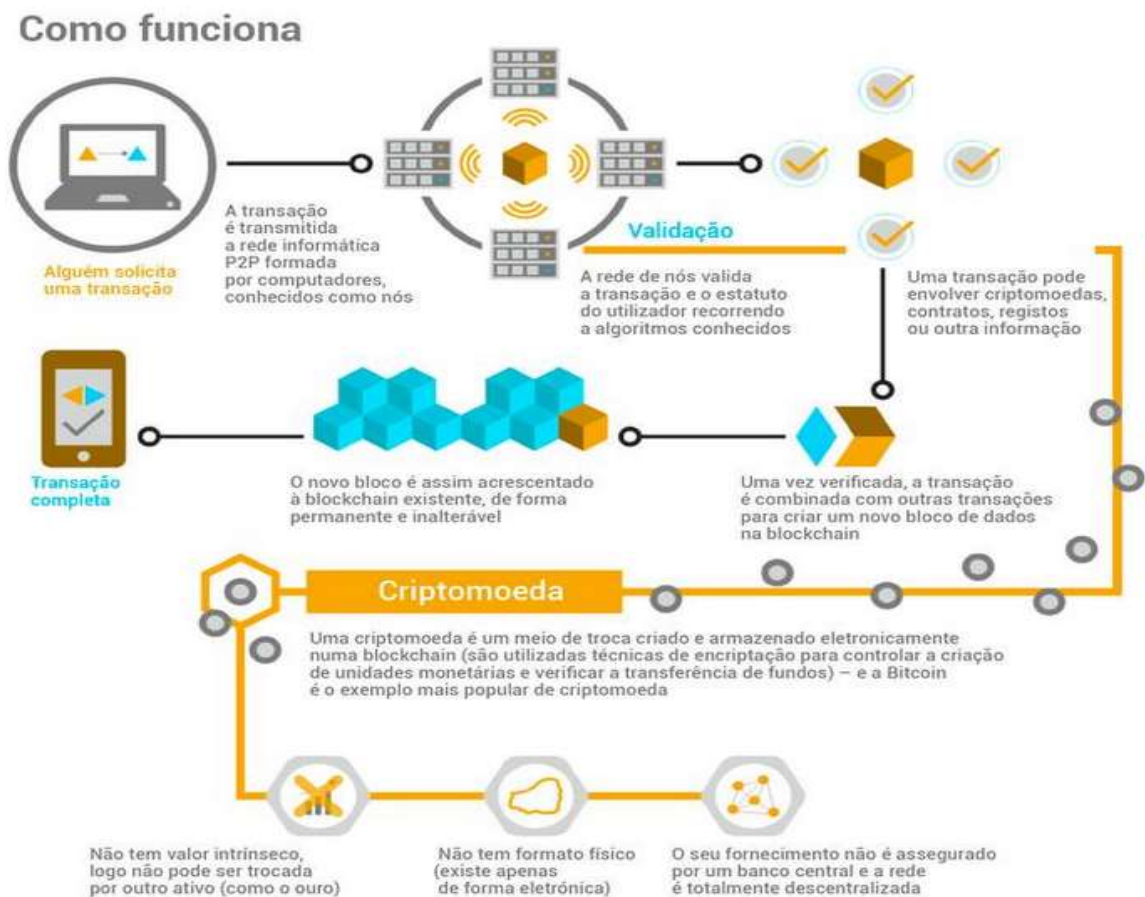
Sendo assim, as criptomoedas não têm um lastro oficial, ou seja, seu valor não está atrelado ao papel moeda, como o dólar, ou a outro tipo de ativo tangível, como o ouro. Elas não são emitidas nem reguladas por uma autoridade monetária.

Ulrich (2014, p. 18-19) traz um exemplo prático de uma transação por meio de Bitcoins:

Quando a Maria decide transferir Bitcoins ao João, ela cria uma mensagem, chamada de “transação”, que contém a chave pública do João, assinando com sua chave privada. Olhando a chave pública da Maria, qualquer um pode verificar que a transação foi de fato assinada com sua chave privada, considerada uma troca autêntica, e que João é o novo proprietário dos fundos.

Isto pode ser graficamente visualizado na Figura 1.

Figura 1 – *Blockchain*, a tecnologia por trás da revolução das moedas digitais.



Fonte: LIVTI (2017).

Por meio dessa cadeia de assinaturas de usuários privados, sem a regulação de um órgão central, sem a participação do Estado, o Bitcoin tornou-se conhecido. Nela, o usuário possui

uma chave privada que dá ao portador a possibilidade exclusiva de disposição sobre eles, inclusive não tendo garantias sobre roubo ou perda (GRZYWOTZ, 2019, p. 106-107, *apud* ESTELLITA, 2020).

O funcionamento das criptomoedas se baseia em uma tecnologia de registro descentralizado, um tipo de “contabilidade”, distribuído em uma rede ponto a ponto de computadores espalhados ao redor do mundo. Toda transação realizada é divulgada para a rede, e somente será aceita após um complexo sistema de validação e de uma espécie de consenso da maioria dos participantes da rede. Com isso, as operações são praticamente irreversíveis, por exemplo: se um proprietário tentar reutilizar ativos já negociados (o chamado “gasto duplo”), a rede de computadores rejeitaria a transação, característica essa que eliminaria a necessidade de um intermediário.

O mercado global de criptomoedas tem um *Market Cap* (capitalização de mercado é o valor total de mercado) estimado em aproximadamente 1 trilhão de dólares. O volume diário movimentado oscila entre 80 e 90 bilhões de dólares.

No ano passado, segundo dados consolidados do Banco Central, esse mercado movimentou cerca de R\$ 300 bilhões no Brasil, por meio das *exchanges* de criptomoedas (plataformas digitais onde é possível comprar, vender, trocar e guardar criptomoedas, muito parecidas com corretoras de valores) (MONEY TIMES, 2022).

Segundo um levantamento da empresa de criptomoedas Triple A, em agosto de 2022 havia no Brasil mais de 16,6 milhões de usuários ativos digitais criptomoedas, ou seja, cerca de 7,75% da população brasileira (AMARO, 2022).

A Receita Federal do Brasil divulgou que qualquer criptoativo com valor de compra igual ou superior a R\$ 5 mil, em nome do contribuinte, até 31 de dezembro do ano anterior, precisa ser declarado (MÁXIMO, 2022). Conforme é possível observar na Figura 2, a partir das declarações de Imposto de Renda recebidas por aquele órgão, o número de declarantes triplicou de um ano para o outro.

Figura 2 – Número de contribuintes pessoa física e pessoa jurídica que declararam ao Imposto de Renda movimento com criptomoedas.



Fonte: AMATO (2022).

As criptomoedas não se restringem ao conhecido Bitcoin. Já em 2016 existiam mais de 800 criptomoedas “flutuando” em mercados globalmente conectados (BURNISKE; TATAR, 2019, p. 51). Algumas criptomoedas alternativas, ou “*altcoins*”, como Omni Layer (MasterCoin), BlackCoin e Monero, são promovidas como mais privadas e seguras que o Bitcoin, e assim, aparentemente mais suscetíveis de uso em atividades ilícitas (DION-SCHWARZ; MANHEIM; JOHSTON, 2019, p. 2).

Desde a primeira criptomoeda criada, o Bitcoin, discute-se como regulamentar, fiscalizar e, também, impedir que essa nova tecnologia seja usada de forma indevida, pois não seria viável tentar inibir o seu uso, haja vista estarem no mundo virtual e descentralizadas.

O Projeto de Lei (PL) nº 4.401/2021 dispõe sobre a prestadora de serviços de ativos virtuais; alterando o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 7.492, de 16 de junho de 1986, e 9.613, de 3 de março de 1998, para incluir a prestadora de serviços de ativos virtuais no rol de instituições sujeitas às suas disposições.

Os principais pontos, seriam:

- Obrigar as *exchanges* a ter Cadastro Nacional de Pessoa Jurídica (CNPJ) no Brasil, registro de operações no Conselho de Controle de Atividades Financeiras (COAF) e cadastro de pessoas politicamente expostas;
- Exigir a segregação do patrimônio dos clientes em relação ao patrimônio das *exchanges*;
- Apresentar incentivos à mineração verde, com vantagens tributárias para quem usar energias alternativas para a mineração e validação de operações em redes que usam tecnologias de registro distribuído (*Distributed Ledger Technologies – DLTs*), ou *blockchains*.

O PL nº 4.401/201 foi aprovado no Senado e, por ocasião da conclusão deste trabalho, encontrava-se em tramitação na Câmara dos Deputados (BRASIL, 2021).

3.1 PRINCIPAIS CARACTERÍSTICAS DAS CRIPTOMOEDAS

O Bitcoin trouxe um modelo inédito de transferência de valores que implementou uma nova forma de transação eletrônica a nível mundial, sem a necessidade de um órgão gestor central.

As moedas virtuais e os meios eletrônicos de pagamentos apresentam um grande crescimento no volume transacional, sendo motivo de preocupação por parte das autoridades engajadas na Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (Enccla),

principalmente justificada pelas seguintes características, apontadas pela Força-Tarefa de Ação Financeira (FATF⁸, *apud* BRASIL, 2017c, p. 1):

- Possibilidade de anonimato no comércio de moedas virtuais na internet;
- Limitada possibilidade de identificação e verificação dos participantes nesse mercado;
- Falta de clareza no que se refere à responsabilidade do monitoramento, supervisão e aplicação de sanções ligadas à prevenção a lavagem de dinheiro e financiamento ao terrorismo;
- Falta de um órgão central supervisor, o que favorece a impunidade;
- Dificuldade ou impossibilidade de rastreamento dos fluxos de trocas;
- Rapidez para transferir valores entre países;
- Aumento substancial do número de pessoas/organizações que utilizam e aceitam pagamento de transações em moeda virtual; e
- Aumento da facilidade de uso das moedas virtuais, com baixo investimento e grande retorno para o criminoso.

As características inerentes ao mercado de criptomoedas deixam clara a existência de potenciais riscos aos usuários e investidores. Pois, a criptomoeda independe de legislação e não é restrita a uma só nação ou bloco econômico. Trata-se de uma moeda universal, totalmente virtual, inexistindo simbologia física que represente seu valor econômico.

As características mais relevantes para a diferenciação conceitual entre criptomoedas e outros valores escriturais são: i) serem denominadas na própria unidade de conta; e ii) possuírem estrutura operacional descentralizada, com governança definida primordialmente no *software* por meio do qual funcionam (STELLA, 2017, p. 151).

O Banco Central do Brasil (BCB), por meio de seu Comunicado 31.379, de 16 de novembro de 2017, alerta sobre os riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais, com os seguintes destaques:

(...) estas não são emitidas nem garantidas por qualquer autoridade monetária, por isso não têm garantia de conversão para moedas soberanas, e tampouco são lastreadas em ativo real de qualquer espécie, ficando todo o risco com os detentores. Seu valor decorre exclusivamente da confiança conferida pelos indivíduos ao seu emissor.

(...) se utilizadas em atividades ilícitas, podem expor seus detentores a investigações conduzidas pelas autoridades públicas visando a apurar as responsabilidades penais e administrativas (BRASIL, 2017b).

O Comunicado esclarece ainda que as empresas que negociam ou guardam as moedas virtuais não são reguladas, autorizadas ou supervisionadas pelo BCB e ressalta que as operações

⁸ *Financial Action Task Force.*

de câmbio com essas moedas não afastam a obrigatoriedade da observância das normas cambiais vigentes.

Em 2018, a Comissão de Valores Mobiliários (CVM) alertou para os seguintes riscos inerentes a investimentos em moedas virtuais, em especial no que diz respeito a emissores ou ofertas não registradas naquela Instituição:

- I.Risco de fraudes e esquemas de “pirâmides financeiras”;
- II.Inexistência de processos formais de adequação do perfil do investidor ao risco do empreendimento;
- III.Risco de operações de lavagem de dinheiro e evasão fiscal ou de divisas;
- IV.Prestadores de serviços atuando sem observar a legislação aplicável;
- V.Material publicitário de oferta que não observa a regulamentação da CVM;
- VI.Riscos operacionais em ambientes de negociação não monitorados pela CVM;
- VII.Riscos cibernéticos (dentre os quais, ataques à infraestrutura, sistemas e comprometimento de credenciais de acesso dificultando o acesso aos ativos ou a perda parcial ou total dos mesmos) associados à gestão e custódia dos ativos virtuais;
- VIII.Risco operacional associado a ativos virtuais e seus sistemas;
- IX.Volatilidade associada a ativos virtuais;
- X.Risco de liquidez (ou seja, risco de não encontrar compradores/vendedores para certa quantidade de ativos ao preço cotado) associado a ativos virtuais; e
- XI.Desafios jurídicos e operacionais em casos de litígio com emissores, inerentes ao caráter virtual e transfronteiriço das operações com ativos virtuais (BRASIL, 2018a).

A Receita Federal do Brasil considera como criptoativos:

Representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal (BRASIL, 2019).

A gestão, criação e circulação da criptomoeda não possui qualquer meio de fiscalização ou supervisão por parte de qualquer órgão regulamentador. A negociação é feita em plataformas eletrônicas ou bilateralmente. A propriedade dos criptoativos é verificada por meio de uma senha, o que dificulta identificar o autor das transações. Nestas condições, o mercado de criptomoedas tem sido objeto frequente de fraudes cometidas por criminosos que são atraídos pelo perfil transfronteiriço das operações, pelo anonimato e por outras particularidades desse mercado.

Dentre os países no entorno estratégico brasileiro, Venezuela e Peru destacam-se como os de maior utilização de criptomoedas, em termos de volume de transações P2P (HAIG, 2019) e densidade populacional de usuários (BUCHHOLZ, 2021), respectivamente.

No ano de 2018 a FATF desenvolveu pesquisas e divulgou plano de trabalho acerca do uso de criptomoedas no financiamento do terrorismo, culminando com a expedição de uma declaração conjunta por parte dos Ministros das Finanças e Presidentes dos Bancos Centrais do grupo das 20 maiores economias do mundo (G20), na qual se comprometiam a implementar os padrões da FATF relacionados a criptoativos (FINANCIAL ACTION TASK FORCE, 2018, p. 23).

Em 2019, na reunião da Enccla em que esteve presente, Santana (2020, p. 16) relata que foi realizada apresentação acerca das criptomoedas estarem sendo utilizadas para financiamento de crimes transnacionais com repercussão para a Segurança Nacional como tráfico de drogas, de armas, de minerais e contrabando de diversas coisas, inclusive animais.

Durante aula para o Curso de Altos Estudos em Defesa em 23 de junho de 2022, o Perito Criminal Federal Philip Villar Mccomish⁹ mencionou já existir comprovação, em investigações internacionais, da utilização de criptomoedas no financiamento ao terrorismo. Todavia, não foram informados detalhes por razões de sigilo.

4 IMPACTOS PARA A SEGURANÇA E A DEFESA NACIONAIS

A utilização de criptomoedas como meio de troca, devido à facilidade com que cada pagamento global pode ser realizado e a percepção entre os usuários de que essas transações são anônimas, pode ameaçar a Segurança Nacional à medida que viabiliza fluxos financeiros ilegais ou não regulamentados, colocando em xeque a Soberania Monetária; esta, no sentido jurídico, pode ser definida como “a capacidade de cada Estado Nacional de emitir sua própria moeda e de impô-la dentro de suas fronteiras, definindo as leis para sua aceitação e seu uso em geral – realizar pagamentos, recolher impostos, denominar preços e contratos, etc” (LAPLANE, 2016, p. 2). Tal desafio à Soberania pode partir tanto de entes intranacionais como de outros Estados.

Nos termos da edição 2020 da Política Nacional de Defesa, atualmente em processo de aprovação no Congresso Nacional, a Segurança Nacional é:

⁹ Lotado na Coordenação de Enfrentamento ao Terrorismo da Diretoria de Inteligência Policial da Polícia Federal.

Entendida como a condição que permite a preservação da soberania e da integridade territorial, a realização dos interesses nacionais, a despeito de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais (BRASIL, 2020, p. 11).

A partir dessa definição, percebe-se que o Combate do Financiamento ao Terrorismo, no contexto da Guerra Global ao Terrorismo declarada pelos EUA, passou por um processo de securitização¹⁰ em diversos Estados, o que acarretou no engajamento de unidades especializadas das respectivas Forças Armadas.

Ainda que tal processo não tenha ocorrido ao Brasil, estando o tratamento da ameaça no campo da gestão político-administrativa, a Política Nacional de Inteligência em vigor destaca a necessidade de colaboração internacional:

O Brasil solidariza-se com os países diretamente afetados por este fenômeno, condena enfaticamente as ações terroristas e é signatário de todos os instrumentos internacionais sobre a matéria. Implementa as resoluções pertinentes do Conselho de Segurança da Organização das Nações Unidas. A temática é área de especial interesse e de acompanhamento sistemático por parte da Inteligência em âmbito mundial.

A prevenção e o combate a ações terroristas e a seu financiamento, visando a evitar que ocorram em território nacional ou que este seja utilizado para a prática daquelas ações em outros países, somente serão possíveis se realizados de forma coordenada e compartilhada entre os serviços de Inteligência nacionais e internacionais e, em âmbito interno, em parceria com os demais órgãos envolvidos nas áreas de defesa e segurança (BRASIL, 2016b, p. 6).

Tais esforços propiciam razão para cooperação entre agências de Inteligência de diferentes países, de forma a fazer frente ao caráter transnacional das redes terroristas modernas.

Mccomish (2022) mencionou que o Comando de Defesa Cibernética¹¹ tem sido um parceiro fundamental da Polícia Federal na repressão aos crimes cibernéticos, que eventualmente poderia incluir os conexos ao terrorismo.

Mais do que a securitização do terrorismo, vemos esta ameaça cada vez mais com a perspectiva de constar na pauta das preocupações da Defesa Nacional. O tema, no Brasil, se coaduna com os seguintes Objetivos Nacionais de Defesa, previstos na Política Nacional de

¹⁰ Segundo Barry Buzan, Ole Wæver e Jaap de Wilde, na obra “*Security: A new Framework for Analysis*” (apud QUEIROZ, 2022), Securitização pode ser entendida como um processo extremo de politização, no qual o ator securitizador, diante de uma situação de ameaça, busca colocar o objeto a ser protegido em um lócus de decisão imune às regras ordinárias do jogo político em que se justificaria, portanto, a utilização dos meios necessários para resolver o problema.

¹¹ Comando Conjunto permanentemente ativado, liderado pelo Exército Brasileiro.

Defesa (PND) encaminhada pelo Ministério da Defesa, em 22 de julho de 2020, para apreciação do Congresso Nacional¹²:

- VII. Contribuir para a estabilidade regional e para a paz e a segurança internacionais; e
- VIII. Incrementar a projeção do Brasil no concerto das Nações e sua inserção em processos decisórios internacionais (BRASIL, 2020, p. 25).

O tema também comporta as seguintes Ações Estratégicas de Defesa previstas na Estratégia Nacional de Defesa (END), também remetida ao Congresso Nacional em 2020:

- AED-5 Fortalecer o Sistema Brasileiro de Inteligência;
- AED-24 Incrementar as capacidades das Forças Armadas para atuar em operações interagências;
- AED-25 Incrementar as capacidades das Forças Armadas para contribuir na prevenção e no enfrentamento às redes criminosas transnacionais;
- AED-60 Capacitar as Forças Armadas para cooperar com os órgãos públicos;
- AED-82 Intensificar a atuação em foros multilaterais e em mecanismos inter-regionais; e
- AED-85 Aperfeiçoar o adestramento de civis e militares para participação em operações internacionais (BRASIL, 2020, p. 63-75).

No plano internacional, observa-se o engajamento direto de Comandos Combatentes dos EUA na repressão do financiamento ao terrorismo (UNITED STATES OF AMERICA, 2021, p. 6). Nesta atividade, Harsono (2020, p. 154) destaca a preeminência do Comando de Operações Especiais (*USSOCOM*, da sigla em inglês) em relação aos demais Comandos Combatentes, manifestando que as Forças de Operações Especiais dos EUA possuem as ferramentas necessárias para moldar o campo de batalha digital e desenvolver as ações apropriadas para a obstrução do financiamento digital para ameaças à Segurança Nacional.

No Brasil, o Glossário das Forças Armadas define Operações Especiais como:

Operações conduzidas por forças militares, especialmente organizadas, adestradas e equipadas, visando a consecução de objetivos políticos, econômicos, psicossociais ou militares relevantes, preponderantemente, por meio de alternativas militares não convencionais. Podem ser conduzidas tanto em tempo de paz quanto em períodos de crise ou conflito armado; em situações de normalidade ou não normalidade institucional; de forma ostensiva, sigilosa ou coberta; em áreas negadas, hostis ou politicamente sensíveis; independentemente ou em coordenação com operações realizadas por forças convencionais; em proveito de comandos de nível estratégico, operacional ou tático (BRASIL, 2015, p. 196).

¹² Preferiu-se referenciar as propostas da Política Nacional de Defesa e da Estratégia Nacional de Defesa em trâmite, em vez dos documentos em vigor, elaborados em 2016 e aprovados pelo Congresso Nacional em 2018, a fim de conferir maior atualidade à pesquisa, considerando-se a rápida evolução do tema em paralelo à aceleração tecnológica. Os documentos foram publicados na página do Ministério da Defesa na internet (BRASIL, 2020).

Segundo Dudley (2021, p. 272-276), o uso da tecnologia *blockchain* em nível estatal, por parte de adversários dos EUA, teria o potencial de viabilizar sistemas econômicos desconectados do sistema baseado no Dólar Estadunidense. Tal possibilidade ameaçaria a expressão econômica do Poder Nacional dos EUA, e assim justificaria o enfrentamento da ameaça sob o prisma da Defesa Nacional. Venezuela, Irã, Rússia e Coreia do Norte já estariam utilizando criptomoedas como meio de evasão de sanções econômicas dos EUA e viabilizar participação no comércio-internacional.

Em resposta a pergunta formulada durante o 1º Simpósio de Segurança Cibernética da Escola Superior de Defesa, em 9 de junho de 2022, o conferencista Marcelo Paiva Fontenele¹³ mencionou que as criptomoedas são utilizadas comumente em pedidos de resgate negociados por criminosos praticantes de *ransomware*, e que existe uma tendência de alguns Estados em tratar tal modalidade de ataque cibernético, a depender do alvo (como infraestruturas críticas), como terrorismo.

Ransomware pode ser entendido como um código malicioso que infecta dispositivos computacionais com o objetivo de sequestrar, capturar ou limitar o acesso aos dados ou informações de um sistema, geralmente através da utilização de algoritmos de encriptação (*crypto-ransomware*), para fins de extorsão. Para obtenção da chave de decifração, geralmente é exigido o pagamento (*ransom*) através de métodos online, como criptomoedas (BRASIL, 2017a).

Um exemplo de ataque por *ransomware* a infraestrutura crítica, ocorrido no Brasil em 2019, foi a paralisação do porto de Mucuripe, em Fortaleza por mais de uma semana, devido à invasão de vários sistemas da Companhia Docas do Ceará, dentre os quais o utilizado para controle das operações portuárias e cobrança de faturas (BRASILINE TECNOLOGIA, 2019). Outro exemplo, agora nos EUA, foi a interrupção de um oleoduto da companhia Colonial Pipeline, em 2021. Apesar de em ambos os casos as ocorrências não terem sido enquadradas como crime de terrorismo, o incidente estadunidense elevou o debate acerca dos riscos do *ransomware* para a Segurança Nacional (GURA, 2021).

Aqui retorna-se à falta de pleno consenso internacional quanto às definições sobre terrorismo, à medida que um Estado pode adaptá-la conforme suas conveniências políticas e estratégicas. Nesta linha de pensamento verifica-se a dicotomia, amplamente citada na literatura

¹³ Coronel do Exército Brasileiro, Diretor do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), PhD em Cibernética -Universidade de Reading, Reino Unido.

especializada no estudo do fenômeno em tela, segundo a qual “o terrorista de um pode ser o lutador pela liberdade de outro” (BAKKER; VAN ZUIJDEWIJN, 2018, p. 1).

É válido inferir que as mesmas características que tornam as criptomoedas atrativas para o financiamento ao terrorismo tornam interessantes reflexões quanto ao emprego no contexto de Guerra Híbrida e “táticas de Zona Cinza”. Hoffman (2018, p. 36) define a primeira como:

A aplicação proposital, e sob medida, de capacidades militares avançadas com táticas irregulares, com terrorismo e atividades criminais, ou a combinação de forças regulares e irregulares, operando como parte de um desenho comum no mesmo espaço de batalha¹⁴.

O mesmo autor (2018, p. 40) define “táticas de Zona Cinza” como:

Atividades veladas ou ilegais, atípicas ao Estado de Direito, situadas em nível inferior ao da violência organizada; incluem: perturbação da ordem, subversão política de organizações governamentais e não-governamentais, operações psicológicas, abuso de processos legais e corrupção financeira, como parte de um desenho integrado para obter vantagem estratégica¹⁵.

Retomando o raciocínio a respeito de alegados “lutadores pela liberdade” cuja causa seja do interesse de determinado Estado apoiar, tais combatentes poderiam ser financiados por meio de criptomoedas, de forma a: descaracterizar o envolvimento estatal, tornar plausível a negação de interferência oficial ou sobrepujar mecanismos de bloqueio financeiro implantados pelo adversário.

Constata-se, assim, que atividades relacionadas a Operações Especiais poderiam ser facilitadas mediante tais procedimentos, como, por exemplo, o pagamento de informantes, que dessa forma seria mais eficiente do que pagamentos realizados em dinheiro vivo (NANDAKUMAR; CEDERQUIST, 2021, p. 284).

5 CONSIDERAÇÕES FINAIS

¹⁴ Tradução do original: “*The purposeful and tailored violent application of advanced conventional military capabilities with irregular tactics, with terrorism and criminal activities, or combination of regular and irregular forces, operating as part of a common design in the same battlespace*”.

¹⁵ Tradução do original: “*Those covert or illegal activities of non-traditional statecraft that are below the threshold of armed organized violence; including disruption of order, political subversion of government or non-governmental organizations, psychological operations, abuse of legal processes, and financial corruption as part of an integrated design to achieve strategic advantage*”.

Criptomoedas são ativos independentes que não têm um valor intrínseco, nem uma centralização como os bancos fazem com a moeda oficial do país. Elas são transacionadas entre os usuários, por meio de redes computacionais, para o registro e a validação das transações. A percepção e a flutuação de seu valor são resultantes de movimentos de oferta e demanda no mercado.

O interesse por criptomoedas é crescente no mundo e no mercado brasileiro, como é possível evidenciar pelos valores movimentados e pelo crescimento do número de contribuintes declarado à Receita Federal. O poder público segue o movimento dos consumidores e avança, tanto na criação de legislação e de normativos infralegais para dar maior segurança jurídica e tratamento tributário aos usos de criptoativos, quanto na regulação dos agentes que operam nesse mercado.

O fato de não haver fronteiras para a negociação das criptomoedas facilita o cometimento de ilícitos. Ao contrário do que acontece no branqueamento de capitais, em que o objetivo é a ocultação da origem do dinheiro, no financiamento do terrorismo o principal propósito é o de encobrir a finalidade a que destinam os recursos. Neste contexto, como a circulação de criptomoedas é global, a cooperação precisa ser internacional.

No Brasil, conquanto a repressão do financiamento ao terrorismo por criptomoedas seja, em princípio, tema de Segurança Pública, capitaneado pela Polícia Federal, considera-se que conhecimentos a respeito da tecnologia *blockchain* e do desenvolvimento de técnicas e procedimentos associados, também seriam úteis ao Ministério da Defesa e às Forças Armadas, identificando-se a possibilidade de envolvimento dos respectivos órgãos de Inteligência, do Comando de Defesa Cibernética e de Forças Especiais¹⁶.

Isto fica ainda mais evidente ante a possibilidade da realização de ataques de *ransomware* contra infraestruturas críticas ou de Defesa Nacional, nos quais usualmente os pedidos de resgate ocorrem por meio de criptomoedas.

Assim, a resposta à pergunta de pesquisa apresentada na introdução deste trabalho indica a necessidade de contínua e incremental integração entre órgãos civis de Segurança e Forças Armadas, com ênfase na Atividade de Inteligência, tanto no âmbito internacional como no nacional, para o enfrentamento do uso de criptomoedas como meio de financiamento ao terrorismo.

¹⁶ “Tropa de operações especiais apta na condução de guerra irregular, que, pela versatilidade que lhe confere a estrutura, o grau de instrução e o grande número de especialistas, pode ser empregada em grande variedade de missões que contribuem para a consecução dos objetivos da força como um todo” (BRASIL, 2015, p. 125).

Entende-se que tal sinergia de esforços contribuirá para o fortalecimento da Defesa Nacional, tanto sob o aspecto defensivo, ante “táticas de Zona Cinza” que venham a ser adotadas por forças adversas, em ambiente de Guerra Híbrida, como podem aperfeiçoar doutrinas de emprego das Forças Especiais brasileiras.

A principal limitação à pesquisa foi a impossibilidade de acessar ou contemplar informações classificadas, como as afetas a investigações policiais, operações conjuntas e inter-agências. Os autores também resguardaram informações protegidas por sigilo funcional.

Longe de esgotar o assunto, contudo, sugere-se que este trabalho sirva como oportunidade para o aprofundamento das análises apresentadas e estudo de temas relacionados, como a canalização de recursos por meio de criptomoedas para o financiamento de conflitos armados, a exemplo do ocorrido entre Rússia e Ucrânia no ano de elaboração deste artigo, bem como a ponderação sobre a possibilidade de aperfeiçoamento legislativo acerca do limite a partir do qual um ataque de *ransomware* poderia ser enquadrado como ato terrorista.

REFERÊNCIAS

AMARO, Lorena. **Brasil é o 7º país do mundo em adoção de criptomoedas, revela pesquisa**. 25 ago. 2022. [São Paulo]: CriptoFácil, 2022. Disponível em: <https://www.criptofacil.com/brasil-e-o-7o-pais-do-mundo-em-adocao-de-criptomoedas-revela-pesquisa/>. Acesso em: 28 set. 2022.

AMATO, Fábio. Operações com criptomoedas mais que dobram e atingem R\$ 200,7 bilhões em 2021, diz Receita. 2022. **G1 Economia**, Brasília, DF, 17 fev. 2022. Disponível em: <https://g1.globo.com/economia/noticia/2022/02/17/operacoes-com-criptomoedas-mais-que-dobram-e-atingem-r-2007-bilhoes-em-2021-diz-receita.ghtml>. Acesso em: 25 set. 2022.

BAKKER, Edwin; VAN ZUIJDEWIJN, Jeanine de Roy. Are returning foreign fighters future terrorists? *In*: JACKSON, Richard; PISOIU, Daniela (ed.). **Contemporary Debates on Terrorism**. 2. ed. New York: Routledge, 2018. Cap. 9. p. 131-146. Disponível em: <https://scholarlypublications.universiteitleiden.nl/access/item%3A3192039/view>. Acesso em: 26 set. 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 02 jul. 2022.

BRASIL. Lei nº 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. **Diário Oficial da União**. Brasília, DF: Imprensa Nacional, 4 mar. 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L9613.htm. Acesso em: 25 set. 2022.

BRASIL. Ministério da Defesa. **MD35-G-01**: Glossário das Forças Armadas. 5ª ed. Brasília, DF: Estado-Maior Conjunto das Forças Armadas, 2015. 294 p. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35-G-01-glossario-das-forcas-armadas-5-ed-2015-com-alteracoes.pdf>. Acesso em: 1º maio 2022.

BRASIL. Lei nº 13.260, de 16 de março de 2016. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis nº 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. **Diário Oficial da União**. Brasília, DF: Imprensa Nacional, 18 mar. 2016a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em: 7 ago. 2022.

BRASIL. Decreto nº 8.793, de 26 de junho de 2016b. Fixa a Política Nacional de Inteligência. **Diário Oficial da União**. 124. ed. Brasília, DF: Imprensa Nacional, 30 jun. 2016b. Seção 1, p. 5-6. Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=30/06/2016&jornal=1&pagina=6&totalA>. Acesso em: 24 abr. 2022.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. **Alerta nº 07/2017**: ataques de *ransomware Bad Rabbit*. Brasília, DF: Centro de Tratamento de Incidentes de Redes do Governo, 2017a. Disponível em: https://www.gov.br/ctir/pt-br/centrais-de-conteudo/publicacoes/alertas/2017/alerta_2017_07_ransomwarebadrabbit.pdf. Acesso em: 25 set. 2022.

BRASIL. Banco Central. **Comunicado nº 31.379**, de 16 de novembro de 2017. Alerta sobre os riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais. Brasília, DF, 16 nov. 2017b. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=31379>. Acesso em: 25 set. 2022.

BRASIL. Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro. **Moedas Virtuais e Meios Eletrônicos de Pagamento**: Tipologias. Brasília, DF: Secretaria Executiva da Enccla, 30 nov. 2017c. Versão 3.0. Disponível em: <http://enccla.camara.leg.br/acoes/arquivos/resultados-enccla-2017/moedas-virtuais-tipologias/view>. Acesso em: 16 nov. 2022.

BRASIL. Comissão de Valores Mobiliários. **CVM esclarece que não faz recomendação ou ratifica ofertas de criptomoedas Initial Coin Offerings (ICOs)**. Rio de Janeiro, RJ, 7 mar. 2018a. Disponível em: https://www.investidor.gov.br/noticias/2018_03_07.html. Acesso em: 16 nov. 2022.

BRASIL. Decreto Legislativo nº 179, de 14 de dezembro de 2018. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, encaminhados ao Congresso Nacional pela Mensagem (CN) nº 2 de 2017 (Mensagem nº 616, de 18 de novembro de 2016, na origem). **Diário Oficial da União**. Brasília, DF: Imprensa Nacional, 17 dez. 2018b. Seção 1, p. 4. Disponível em: <https://www2.camara.leg.br/legin/fed/decleg/2018/decretolegislativo-179-14-dezembro-2018-787452-publicacaooriginal-156961-pl.html>. Acesso em: 28 set. 2022.

BRASIL. Receita Federal. Instrução Normativa RFB nº 1888, de 3 de maio de 2019. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). **Diário Oficial da União**. Brasília, DF: Imprensa Nacional, 7 mai. 2019. Seção 1, p. 14. Disponível em: <https://in.gov.br/web/dou/-/instru%C3%87%C3%83o-normativa-n%C2%BA-1.888-de-3-de-maio-de-2019-87070039>. Acesso em: 24 out. 2022.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa (PND) e Estratégia Nacional de Defesa (END) encaminhadas para apreciação do Congresso Nacional**. Brasília, DF, 22 jul. 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/estrategia-nacional-de-defesa. Acesso em: 25 set. 2022.

BRASIL. **Projeto de Lei nº 4401, de 2021**. Dispõe sobre a prestadora de serviços de ativos virtuais; e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 7.492, de 16 de junho de 1986, e 9.613, de 3 de março de 1998, para incluir a prestadora de serviços de ativos virtuais no rol de instituições sujeitas às suas disposições. Brasília, DF, 26 mai. 2022. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/151264>. Acesso em: 28 set. 2022.

BRASILINE TECNOLOGIA. **Porto de Fortaleza completa uma semana refém de ciberataque**. [S.l.], 6 nov. 2019. Disponível em: <https://brasiline.com.br/blog/porto-de-fortaleza-completa-uma-semana-refem-de-ciberataque/>. Acesso em: 27 set. 2022.

BUCHHOLZ, Katharina. **How Common is Crypto?** 17 mar. 2021. [S.l.]: Statista. Disponível em: <https://www.statista.com/chart/18345/crypto-currency-adoption/>. Acesso em: 11 ago. 2022.

BURNISKE, Chris; TATAR, Jack. **Criptoativos: o guia do investidor inovador para o Bitcoin e além**. Rio de Janeiro: Alta Books, 2019.

CHUY, José Fernando M. **Operação Hashtag: a primeira condenação de terroristas islâmicos na América Latina**. Barueri, SP: Novo Século Editora, 2018.

DION-SCHWARZ, Cynthia; MANHEIM, David; JOHSTON, Patrick B. (org.). **Terrorist Use of Cryptocurrencies: technical and organizational barriers and future threats**. Santa Monica, Calif: RAND Corporation, 2019. 99 p. Disponível em: https://www.rand.org/pubs/research_reports/RR3026.html. Acesso em: 31 jul. 2022.

DUCRÉE, Jens. **Satoshi Nakamoto and the Origins of Bitcoin: the profile of a 1-in-a-billion genius**. [S.l.], 2022. Disponível em: <https://arxiv.org/abs/2206.10257>. Acesso em: 27 set. 2022.

DUDLEY, Sara. Cryptocurrency: will the digitization of currency allow malign actors to achieve strategic effects? *In*: DAVIS, Zachary S. *et al* (ed.). **Strategic Latency Unleashed: the role of technology in a revisionist global order and the implications for Special Operations Forces**. Livermore, USA: Center For Global Security Research Lawrence Livermore National Laboratory, 2021. Cap. 19. p. 269-282. Disponível em: <https://cgsr.llnl.gov/content/assets/docs/StratLatUnONLINE.pdf>. Acesso em: 8 ago. 2022.

ESTELLITA, Heloisa. Criptomoedas e lavagem de dinheiro. Resenha de: GRZYWOTZ, Johanna. *Virtuelle Kryptowährungen und Geldwäsche*. Berlin: Duncker & Humblot, 2019. **Revista Direito GV**, v. 16, n. 1. São Paulo, SP, jan./abr. 2020,. DOI: <http://dx.doi.org/10.1590/2317-6172201955>.

FINANCIAL ACTION TASK FORCE. **FATF Annual Report 2017-2018**. Paris, p. 78. 2018. Disponível em: <https://www.fatf-gafi.org/publications/fatfgeneral/documents/annual-report-2017-2018.html>. Acesso em: 13 jun. 2022.

FONTENELE, Marcelo Paiva. Os desafios da Segurança Cibernética no mundo contemporâneo, em particular, no Brasil. *In*: SIMPÓSIO DE SEGURANÇA CIBERNÉTICA DA ESCOLA SUPERIOR DE DEFESA, 1º, 2022. Brasília, DF. [Anais]. Brasília: ESD, 2022.

GURA, David. **U.S. suffers over 7 ransomware attacks an hour. It's now a National Security risk**. 9 jun. 2021. [S.l.]: NPR, 2021. Disponível em: <https://www.npr.org/2021/06/09/1004684788/u-s-suffers-over-7-ransomware-attacks-an-hour-its-now-a-national-security-risk>. Acesso em: 27 set. 2022.

HAIG, Samuel. **P2P Markets: Russian Local Bitcoins Trade Outpaces Venezuela**. 8 mar. 2019. [S.l.]: Bitcoin.com, 2019. Disponível em: <https://news.Bitcoin.com/russian-localBitcoins-trade-outpaces-venezuela/>. Acesso em: 11 ago. 2022.

HARSONO, Hugh. Prioritizing SOF Counter-Threat Financing Efforts in the Digital Domain. **The Cyber Defense Review**, West Point, NY, USA, v. 5, n. 3, p. 153-159, Fall 2020. Quarterly. Disponível em: https://cyberdefensereview.army.mil/Portals/6/Documents/2020_fall_cdr/CDR%20V5N3%2010_Harsono.pdf?ve. Acesso em: 4 maio 2022.

HE, Dong *et al* (ed.). **Virtual Currencies and Beyond**: initial considerations. [S.l.]: International Monetary Fund, 2016. Disponível em: <https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Virtual-Currencies-and->. Acesso em: 25 set. 2022.

HOFFMAN, Bruce. Rethinking Terrorism and Counterterrorism Since 9/11. **Studies In Conflict & Terrorism**, Arlington, VA, USA, v. 25, n. 5, p. 303-316, set. 2002. Disponível em: <https://www.tandfonline.com/doi/pdf/10.1080/105761002901223>. Acesso em: 5 ago. 2022.

HOFFMAN, Frank G. Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. **Prism: The Journal of Complex Operations**, Washington, DC, v. 7, n. 4, p. 30-47, nov. 2018. Disponível em: https://cco.ndu.edu/Portals/96/Documents/prism/prism7_4/181204_Hoffman_PDF.pdf?ver=2018-12-04-161237-307. Acesso em: 28 set. 2022.

INSTITUTE FOR ECONOMICS & PEACE. **Global Terrorism Index 2022**: measuring the impact of terrorism. Sydney: IEP, 2022. Disponível em: <https://www.visionofhumanity.org/resources/>. Acesso em: 28 ago. 2022.

LAPLANE, Ezequiel Greco. Hierarquia de moedas e soberania monetária: uma primeira aproximação. In: ENCONTRO NACIONAL DE ECONOMIA, 44., 2016, Foz do Iguaçu. [Anais]. Niterói: Associação Nacional dos Centros de Pós-Graduação em Economia, 2016. p. 2-2. Disponível em: https://www.anpec.org.br/encontro/2016/submissao/files_I/i7-eee4fa1bd86ad67c66ca6e418af98471.pdf. Acesso em: 28 ago. 2022.

LIVTI. **Blockchain**: a tecnologia por trás das moedas digitais. [Santa Catarina]: 6 out. 2017. Disponível em: <https://www.livti.com.br/blog/blockchain-tecnologia-por-tras-da-revolucao-das-moedas-digitais/>. Acesso em: 25 set. 2022.

LOPES, João do Carmo; ROSSETTI, José Paschoal. **Economia monetária**. 8. ed. São Paulo, SP: Atlas, 2002.

MÁXIMO, Welton. **Agência Brasil explica**: como declarar criptoativos no Imposto de Renda: ativos virtuais a partir de R\$ 5 mil precisam ser informados. 25 abr. 2022. Brasília, DF: Agência Brasil, 2022. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2022-04/agencia-brasil-explica-como-declarar-criptoativos-no-imposto-de-renda>. Acesso em: 30 set. 2022.

MCCOMISH, Philip Villar. **Enfrentamento ao terrorismo e investigações no meio cibernético**. Aula para o Curso de Altos Estudos em Defesa. Brasília, DF: Escola Superior de Defesa, 23 de junho de 2022.

MONEY TIMES. **Marco regulatório das criptomoedas**: rumo à transparência e segurança nas operações brasileiras. rumo à transparência e segurança nas operações brasileiras. 25 ago. 2022. [S.l.], 2022. Disponível em: <https://www.moneytimes.com.br/marco-regulatorio-das-criptomoedas-rumo-a-transparencia-e-seguranca-nas-operacoes-brasileiras/>. Acesso em: 14 nov. 2022.

NAKAMOTO, Satoshi. **Bitcoin**: a peer-to-peer electronic cash system. [S.l.], 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 27 set. 2022.

NANDAKUMAR, Girish Sreevatsan; CEDERQUIST, Jon. Blockchain and the Battlefield. In: DAVIS, Zachary S. *et al* (ed.). **Strategic Latency Unleashed**: the role of technology in a revisionist global order and the implications for Special Operations Forces. Livermore, USA: Center For Global Security Research Lawrence Livermore National Laboratory, 2021. Cap. 20. p. 283-292. Disponível em: <https://cgsr.llnl.gov/content/assets/docs/StratLatUnONLINE.pdf>. Acesso em: 28 set. 2022.

QUEIROZ, Fábio Albergaria de. **A Escola de Copenhague e os estudos em Segurança Internacional**. Aula para o Curso de Altos Estudos em Defesa. Brasília, DF: Escola Superior de Defesa, 9 de junho de 2022.

SANTANA, Vinicius. **A lavagem de dinheiro por meio de criptomoedas e o risco para Defesa Nacional**. 2020. 25 f. TCC (Especialização) - Curso de Altos Estudos em Defesa, Escola Superior de Guerra - Campus Brasília, DF, 2020. Disponível em: <https://repositorio.esg.br/bitstream/123456789/969/1/VINICIUS%20SANTANA%20-%20TCC%20CAED%202020%20v2.pdf>. Acesso em: 25 set. 2022.

SISTEMA Militar de Defesa Cibernética entra em vigor nesta terça-feira. **EPEX - Escritório de Projetos do Exército Brasileiro**, Brasília, DF. 31 nov. 2020. Disponível em: <http://www.epex.eb.mil.br/index.php/ultimas-noticias/1926-sistema-militar-de-defesa-cibernetica-entra-em-vigor-nesta-terca-feira>. Acesso em: 29 set. 2022.

STELLA, Julio Cesar. Moedas Virtuais no Brasil: como enquadrar as criptomoedas. **Revista da Procuradoria-Geral do Banco Central**, Brasília, DF, v. 11, n. 2, p. 149-162, dez. 2017. Disponível em: <https://revistapgbcbcb.gov.br/index.php/revista/issue/view/26/A9%20V.11%20-%20N.2>. Acesso em: 27 set. 2022.

TEIDER, Lucas Hinckel. **Terrorismo e seu financiamento: a política pública criminal brasileira de prevenção**. São Paulo, SP: Editora Dialética, 2021.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo, SP: Instituto Ludwig von Mises Brasil, 2014. Disponível em: <https://produtos.infomoney.com.br/hubfs/ebook-bitcoin.pdf>. Acesso em: 25 set. 2022.

UNITED NATIONS. General Assembly. Resolution 49/60. **Measures To Eliminate International Terrorism**. New York, 17 fev. 1995. Disponível em: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/49/60. Acesso em: 04 ago. 2022.

UNITED STATES OF AMERICA. Department of Defense. Office of Inspector General. Report n. DODIG-2021-082, May 18, 2021. **Evaluation Of Combatant Command Counter Threat Finance Activities**. Alexandria, VA. Disponível em: https://media.defense.gov/2021/May/28/2002731277/-1/-1/1/DODIG-2021-082_REDACTEDV1.PDF. Acesso em: 4 maio 2022.

VAN BUGGENHOUT, Gothardo Backx. Risco do uso das criptomoedas para o financiamento do terrorismo. **Revista de Ciências Jurídicas e Sociais - IURJ**, [S.l.], v. 2, n. 2, p. 45-63, 20 ago. 2021. Disponível em: <http://dx.doi.org/10.47595/cjsiurj.v2i2.46>. Acesso em: 29 ago. 2022.

WILLIAMS, Dodeye Uduak; OKON, Enoch; OBASA, Tony. The Utility of Military Force and the Global War on Terror (GWOT): Strategic or Tactical?. **Journal Of Humanities And Social Policy**, [S.l.], v. 4, n. 2, p. 1-2, jun. 2018. Disponível em: https://www.researchgate.net/profile/Enoch-Okon/publication/331466264_The_Utility_of_Military_Force_and_the_Global_War_on_Terror_GWOT_Strategic_or_Tactical/links/5c7a67e9a6fdcc4715a759b2/The-Utility-of-Military-Force-and-the-Global-War-on-Terror-GWOT-Strategic-or-Tactical.pdf. Acesso em: 28 ago. 2022.