O terrorismo e a dimensão digital dos oceanos: desafios à sociedade

Capitão-de-mar-e-guerra
Helder Fialho de Jesus

1. Introdução*

As ações terroristas abrangem uma ampla variedade de métodos e táticas que refletem tanto a diversidade de objetivos políticos, ideológicos e religiosos dos grupos terroristas quanto o seu desejo de causar o maior impacto possível1. Estas ações têm na sua generalidade três elementos: (1) Atos criminosos – incluindo violência ou ameaça de violência; (2) Intenção – causar destruição, morte, ferimentos graves ou fazer reféns; e (3) Objetivo – incutir medo, intimidar ou coagir governos ou organizações. No contexto da presente reflexão, considera-se que o terrorismo é uma ameaça à segurança e visa provocar o medo e a incerteza coletiva através da violência de uma intenção dolorosa associada, naqueles que podem ser diretamente afetados e, com especial ênfase, através da exposição de imagens transmitidas associadas aos efeitos dos ataques. O efeito psicológico é geralmente mais prevalente do que as lesões físicas de um evento terrorista2, os quais têm associado o baixo custo e o efeito assimétrico, não necessitando de muitos recursos ou técnicas muito complexas. Por sua vez, estes atos podem visar três vertentes:

a. Política – tendo em vista alterar ou influenciar regimes. Os grupos terroristas podem utilizar a violência como um meio de perturbar a governação, prejudicar a confiança nos

sistemas políticos existentes ou pressionar as autoridades através de coerção visando concessões, como Martha Crenshaw aborda no seu livro "Explaining Terrorism". São exemplos o Exército Republicano Irlandês (Irish Republican Army – IRA) na Irlanda do Norte, as Forças Armadas Revolucionárias da Colômbia (FARC) na Colômbia, ou a Pátria Basca e Liberdade (Euskadi Ta Askatasuna – ETA) em Espanha.

b. Social, em três níveis – (1) Religioso – visando estabelecer a supremacia religiosa, impor interpretações rigorosas das leis religiosas ou combater as ameaças percebidas às suas crenças religiosas, como Audrey Kurth Cronin apresenta em "How Terrorism Ends"; (2) Étnico ou nacionalista – de modo a alcançar a autonomia, a independência ou o controlo territorial para um grupo étnico ou nacional específico, onde o livro "Inside Terrorism" de Bruce Hoffman se constitui como um exemplo, ou (3) Ideológico – para efeitos de polarizar comunidades de modo a promover uma ideologia específica, semear discórdia ou intimidar os adversários, conforme Jessica Stern apresenta em "Terror in the Name of God".

c. Económica – destinadas a perturbar as atividades económicas ou a enfraquecer os governos, com ataques de infraestruturas críticas, instituições financeiras ou indústrias relevantes, como Walter Enders e Todd Sandler referem em "The Political Economy of Terrorism", constituindo-se as democracias liberais como alvos preferenciais para os terroristas.

A ação terrorista sobre a dimensão digital, e no caso concreto dos oceanos, tem associado o exercício da disrupção[3] ou da destruição de sistemas, plataformas ou serviços, podendo indicar-se que a vertente económica como a mais plausível, no contexto da presente reflexão, pois os efeitos económicos podem atingir um público maior.

As técnicas empregues por atores criminosos para concretização de ciberataques[4] serão tecnicamente idênticas sendo basicamente distinto o seu objetivo. O modelo Cyber Kill Chain[5], criado pela Lockheed Martin, destina-se à compreensão das ações que através do ciberespaço visam interferir com o normal funcionamento de uma organização. Estas ações podem ter como objetivo último, entre outros, a destruição, a disrupção, o roubo ou visando um resgate, mas as várias etapas que os criminosos têm de percorrer até atingirem o seu fim são idênticas. Este modelo, de sete etapas, fornece informação sobre um ataque e ajuda à compreensão sobre as táticas, técnicas e processos dos atacantes, permitindo assim antecipar a defesa contra ameaças e a prevenção de atividades de intrusão através do ciberespaço. Desta forma, a Cyber Kill Chain[6] constitui-se como uma referência genérica, alterando-se o móbil final, podendo este ser para obtenção de dinheiro ou dividendos, com o cibercrime, para roubo de informação classificada, científica, empresarial ou outra sensível, para efeitos de ciberespionagem, ou para criar medo na sociedade, através de ações terroristas no ciberespaço. No entanto, a inter-relação entre este tipo de atores é grande, pelo que as operações da Interpol estão centradas em quatro programas globais: o cibercrime, o terrorismo, o crime organizado e o crime financeiro e a corrupção[7].

2. Europa, Ciberespaço e Infraestruturas Críticas

A nível europeu, no que à segurança do ciberespaço[8] diz respeito, para se conhecer a documentação associada, podemos encontrar 25 elementos[9], o que não facilita a integração e interpretação simplificada, abrangendo uma grande diversidade de áreas da sociedade. Para o presente documento, no que diz respeito à cibersegurança[10] e à proteção de infraestruturas críticas, podem relevar-se duas diretivas, nomeadamente a NIS (network and information security – segurança das redes e da informação) e a CER (resilience of critical entities – resiliência das entidades críticas)[11], assim como a estratégia de cibersegurança da UE para a década digital[12].

A União Europeia (EU) está comprometida com a sua transformação digital, com um montante de investimento sem paralelo até 2027, incluindo novas políticas tecnológicas e industriais, além de uma agenda de recuperação económica. Esta estratégia, de 2020, tem em vista assegurar uma Internet mundial, livre e aberta com barreiras de segurança firmes, com vista a enfrentar os riscos que se colocam à segurança e aos direitos e liberdades fundamentais das pessoas na Europa. Assenta em três instrumentos principais, nomeadamente instrumentos de regulamentação, de investimento e de política, e destina-se a intervir em três domínios de ação da UE: a) resiliência, soberania tecnológica e liderança; b) criação de capacidade operacional para prevenir, dissuadir e responder; e c) promoção de um ciberespaço mundial e aberto.

A diretiva NIS, promulgada em 2016, foi a primeira legislação a nível da EU sobre cibersegurança, que estabelece um conjunto de medidas para prevenir ciber incidentes na Europa[13]. Esta foi atualizada pela Diretiva NIS2[14], que entrou em vigor em 2023, atualizando o quadro jurídico para acompanhar o aumento da digitalização e para fazer face a um crescente quadro de ameaça no que à cibersegurança diz respeito[15]. Por sua vez, expandiu o âmbito das regras de cibersegurança para novos setores e entidades, melhorando ainda mais as capacidades de resiliência e resposta de incidentes das entidades públicas e privadas, das autoridades competentes e da UE como um todo, devendo os Estados-Membros transpor esta diretiva para o seu quadro jurídico até 17 de outubro de 2024.

A diretiva CER, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção, teve a sua primeira versão em 2008[16], considerando apenas os setores dos transportes e da energia como infraestruturas críticas. Em 2019 foi efetuada uma avaliação desta diretiva, evidenciando a necessidade da sua atualização e reforço das regras existentes, face aos novos desafios que a UE enfrenta, como a ascensão da economia digital, os impactos cada vez maiores das alterações climáticas e as ameaças terroristas[17]. Assim,

"As entidades críticas são entidades que prestam serviços que são indispensáveis à manutenção de funções societais e atividades económicas vitais, da saúde e segurança pública e do ambiente. Estas entidades têm de ser capazes de prevenir, proteger, reagir,

gerir e recuperar em caso de ataques híbridos, catástrofes naturais, ameaças terroristas e emergências de saúde pública." 18

A nova diretiva CER19,20 entrou em vigor a 16 de janeiro de 2023, devendo os Estados-Membros transpô-la para a legislação nacional até 17 de outubro de 2024, e estende-se a 11 setores21. No contexto do presente documento, sobre a dimensão digital dos oceanos, consideraram-se os setores da energia (Off shore), dos transportes (marítimo) e das Infraestruturas digitais.

Para analisar a realidade dos sistemas e da informação juntamente com as infraestruturas críticas, optou-se por uma abordagem holística e interdisciplinar, tendo por base a reflexão de Edgar Morin no seu livro "Introdução ao pensamento complexo". Assim, os três setores acima indicados serão alvo de análise e de apresentação de exemplos de disrupções para a dimensão física e para o ciberespaço.

3. Disrupção de setores críticos nos mares e oceanos

a. Setor Energia

No que diz respeito ao setor da energia, na sua componente marítima, verifica-se que as plataformas offshore constituem-se como alvos de alto valor para ataques, sejam físicos ou no ciberespaço. Isto porque geram energia e rendimento para muitos Estados e é facilmente sentida a ação de um dano grave nestes ativos ao nível da economia, das finanças ou da reputação, entre outras. Neste sentido, podem identificar-se três áreas offshore: as plataformas de extração de petróleo, as plataformas de extração de gás natural e as plataformas de produção de energia eólica.

Como exemplos de disrupções neste setor, apresenta-se para a dimensão física a destruição dos gasodutos Nord Stream, em setembro de 2022, nas águas do Mar Báltico, considerado como o ato de sabotagem mais importante dos tempos modernos22. Este, que decorreu no pós invasão russa da Ucrânia, teve repercussões na UE, na Organização do Tratado do Atlântico Norte (North Atlantic Treaty Organization – NATO) com uma posição do Comité do Atlântico Norte a confirmar que "se trata do resultado de actos de sabotagem deliberados, imprudentes e irresponsáveis"23, no Reino Unido24, nos Estados Unidos da América (EUA)25, na Austrália26, entre outros.

"Na sequência da sabotagem dos gasodutos Nord Stream, é necessário adotar, a nível da União, mais medidas de reforço da resiliência das infraestruturas críticas. Por conseguinte, com base numa proposta da Comissão, o Conselho adotou a Recomendação relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas (Recomendação 2023/C 20/01), que visa o reforço do grau de preparação, a melhoria da resposta e a cooperação internacional neste domínio. A recomendação salienta, nomeadamente, a necessidade de assegurar, a nível da União, uma resposta coordenada e eficaz aos riscos atuais e futuros que se colocam à prestação

de serviços essenciais”27.

Por sua vez, a NATO discutiu este tema na sua cimeira de 2023, em Vilnius, saindo no comunicado final28 que os países aliados estão empenhados em identificar e mitigar vulnerabilidades e dependências estratégicas no que diz respeito às suas infraestruturas críticas e em preparar, dissuadir e defender-se contra a utilização coerciva de energia e outras táticas híbridas por parte de intervenientes estatais e não estatais. Foi ainda acordado em estabelecer o Centro Marítimo da NATO para a Segurança das Infraestruturas Submarinas Críticas no âmbito do Comando Marítimo da NATO (MARCOM). Esta situação foi posteriormente reforçada no ano seguinte, na cimeira do 75.º aniversário da Aliança, em Washington29.

No entanto, o tema do Nord Stream continua em aberto, pois investigações efetuadas pelo jornal Washington Post 30 e pela revista Der Spiegel31 apontam a origem desta disrupção para uma operação de um comando militar ucraniano. Situação que o canal DW posteriormente terá confirmado32, referindo que as autoridades alemãs procuram um cidadão ucraniano que estaria na origem dos ataques de 2022, tendo agido com dois cúmplices. Também nas Nações Unidas se tentou esclarecer e investigar a origem desta disrupção, com uma comissão independente, mas o Conselho de Segurança não aprovou a proposta de resolução33.

Assim, os Estados Unidos tornaram-se um fornecedor crítico de LNG (Liquid Natural Gas – Gás Natural Líquido) para a Europa, com um incremento de importações a representarem 44 por cento em 2022 e 48 por cento em 202334. Complementarmente, a UE teve de fazer investimentos consideráveis em infraestruturas de LNG para fazer face ao aumento das importações. A UE implementou também o plano REPowerEU35 para reduzir a dependência dos combustíveis fósseis russos, promovendo a eficiência energética, as energias renováveis e novas cadeias de abastecimento de LNG de países como os EUA, a Noruega, a Argélia e o Qatar. Por sua vez é pouco provável um retorno a esta opção de dependência russa36,37. Relativamente à Alemanha, esta situação teve um impacto significativo na Ostpolitik alemã, iniciada pelo chanceler Willy Brandt, e que teve a sua continuidade mais recente com a chanceler Angela Merkel, visando as boas relações internacionais. Mas os sinais já tinham sido dados anteriormente, aquando da visita do chanceler Olaf Scholz a Washington, em 7 de fevereiro de 2022, tendo sido um tema sobre o qual o presidente Biden também se referiu38, em resposta a jornalistas, confirmando que se a Rússia invadisse a Ucrânia, não haveria Nord Stream239. De relevar que esta sabotagem mostra que o ataque a infraestruturas críticas para fins militares já não está confinado aos limites geográficos de uma zona de conflito.

Como exemplo de uma disrupção no ciberespaço a uma infraestrutura de energia, tem-se o caso do ciberataque à Aramco40, em 2012, uma das maiores empresas de hidrocarbonetos do mundo. Esta situação decorreu tendo por base o vírus Shamoon, o qual se conseguiu espalhar pelos computadores da rede, infetando mais de 30.000 computadores, revelando uma natureza altamente destrutiva, tornando os computadores infetados inutilizáveis. Para responder a este ataque, a empresa desligou-se da Internet para evitar que o vírus se espalhasse ainda mais. Como resultado, os seus sistemas

informáticos estiveram offline durante cerca de duas semanas41. Durante este período, a produção de petróleo e as operações principais da Aramco não foram significativamente perturbadas, uma vez que estes sistemas foram isolados da rede corporativa que foi afetada. No entanto, muitos processos administrativos e não críticos de negócio foram interrompidos. A origem do ataque foi imputada a um grupo chamado 'Cutting Sword of Justice', o qual assumiu a responsabilidade por esta ação, tendo os responsáveis dos serviços de informações dos EUA considerado que o verdadeiro perpetrador do ataque seria o Irão.

b. Setor Transportes

O setor dos transportes marítimos é responsável pelo transporte de cerca de 90% do comércio mundial, constituindo-se como um elemento crítico da economia global42. Sem ele, o comércio intercontinental, o transporte a granel de matérias-primas e a importação/exportação de alimentos e produtos manufaturados a preços acessíveis simplesmente não seriam possíveis. As perspetivas de crescimento desta indústria são fortes e hoje existem mais de 50.000 navios mercantes, transportando todo o tipo de carga. O registo da frota mundial encontra-se distribuída por mais de 150 países, com mais de um milhão de marítimos de praticamente todas as nacionalidades. Por tráfego marítimo43 considera-se todo o transporte marítimo para fins comerciais entre dois ou mais portos ou ancoradouros, com exclusão dos serviços regulares de ferry, navegação de recreio, pesca costeira e transporte fluvial. No contexto do presente documento, considera-se como sistema de transporte marítimo (STM) o sistema de sistemas que incluem o tráfego marítimo (onde se incluem os navios militares), portos, carga e os processos associados (cadeia de abastecimento, movimentação de carga, …).

Para ilustrar a preocupação com esta área e como o ciberespaço é um elemento importante, apresenta-se a Ordem Executiva44 emitida pela Casa Branca para proteger as cadeias de abastecimento vitais e mitigar o risco de ciberataques a infraestruturas críticas, reforçando a autoridade do Departamento de Segurança Interna dos EUA (Department of Homeland Security – DHS) para efeitos de combate às ciberameaças no ambiente marítimo relativamente à segurança das operações, das redes e dos sistemas dos portos dos EUA45.

À semelhança do setor da energia, também no setor dos transportes se apresentam exemplos de disrupções, na dimensão física e no ciberespaço. Relativamente à dimensão física, apresentam-se dois exemplos. Um, na vertente da economia global, com o encalhe do Mega contentor Ever Given no Canal do Suez, em março de 2021, naquela que é uma das rotas comerciais mais movimentadas do mundo, com cerca de 12% do comércio global46. Este acidente, que provocou enormes congestionamentos, teve um custo diário de cerca de 9,6 mil milhões de dólares em mercadorias por dia. O navio, de 200 mil toneladas e operado pela empresa Evergreen Marine, com um comprimento de quatro campos de futebol, é um dos maiores porta-contentores do mundo, com capacidade para transportar 20 mil contentores. O outro exemplo na vertente social, com o porto de

Eilat47, em Israel, onde metade dos trabalhadores deste porto correram o risco de perder os seus empregos, porque o porto de Eilat sofreu um grande golpe financeiro devido à crise nas rotas marítimas do Mar Vermelho, decorrente da ação do grupo terrorista Houthi no Iémen, apoiado pelo Irão, e pelo facto de as companhias de navegação terem redirecionado os navios para evitar os ataques nesta zona.

No ciberespaço são vários os casos de disrupção que têm surgido nos últimos tempos. O custo dos ciberataques em todo o mundo é surpreendente, prevendo-se um valor na ordem dos 10 biliões de dólares até 202548. Embora o transporte marítimo continue a representar uma pequena parte deste total, os ciberataques na indústria marítima estão igualmente a crescer49 e a tornar-se cada vez mais dispendiosos. Dados recentes mostram que um ciberataque custa agora à organização visada uma média de 550.000 dólares. A grande maioria dos ataques, na ordem dos 57%50, encontram-se associados a ramsonware51, no fundo ao cibercrime, para efeitos de resgate.

Como exemplo, entre muitos, apresentam-se três tipos de ataques, sendo um de ataque distribuído de negação de serviço (Distributed Denial of Service – DDOS52) e dois de introdução de malware53, um para efeitos de ciberespionagem e o outro para efeitos de ramsonware. Relativamente ao ataque de DDOS, em 19 de outubro de 2023, vários operadores de ferry europeus sofreram um ciberataque deste tipo, colocando em baixo muitos websites e reservas online. Uma das empresas afetadas foi a Viking Line54, uma empresa de navegação que presta diversos tipos de serviços no Mar Báltico, desde cruzeiros, cargas e transporte de passageiros, com mais de 50 navios e de 2.000 colaboradores. Os sistemas afetados voltaram a estar ativos no dia seguinte. Para o caso de introdução de malware, com o objetivo de ciberespionagem55, a ESET uma consultora de cibersegurança de referência internacional, de origem eslovaca, detetou nos sistemas de várias companhias de navegação na Noruega, na Grécia e nos Países Baixos a existência de um malware chamado Korplug. Esta situação terá decorrido da ação de hackers chineses que conseguiram infiltrar-se de forma persistente na indústria europeia de transporte de carga. Da análise apresentada, este malware poderia estar mesmo a bordo dos navios de carga, e não apenas nos sistemas de escritório utilizados pelo pessoal em terra, tendo alguns casos a sua origem em unidades USB.

Para a última tipologia de ataques, através da introdução de malware, mas para efeitos de regate, indicam-se duas áreas distintas: (1) navios e operadores em terra – na noite de 7 de janeiro de 2023, cerca de 1.000 navios foram afetados por um ataque de ransomware, forçando ao encerramento de servidores56. Um dos casos foi com a DNV, com sede em Oslo e que é a maior sociedade classificadora do mundo, gerindo as certificações técnicas para a construção e operação de navios e estruturas offshore. Mais de 13.175 navios e unidades móveis offshore são atualmente servidas pela DNV. Por sua vez, o também o Porto de Lisboa foi alvo de ataque pelo grupo de ransomware LockBit, em dezembro de 2022, não afetando a sua atividade operacional57; (2) Estaleiros de construção naval – o outro exemplo prende-se com a construção de navios, onde o Fincantieri Marine Group, a parte americana da empresa italiana de construção naval Fincantieri, um dos fabricantes de navios para a Marinha dos EUA, foi alvo de ciberataque em abril de 2023 tendo a informação de quase 17.000 pessoas sido

exposta58. Esta situação foi confirmada levando a "uma interrupção temporária em certos sistemas informáticos na sua rede". No entanto, numa empresa que constrói os navios de combate litoral da classe Freedom e as fragatas de mísseis guiados da classe Constellation, as máquinas responsáveis pela soldadura, corte e muito mais ficaram em baixo durante dias depois, de os servidores terem sido desligados. Esta situação não é nova pois um outro construtor para a Marinha dos EUA, a Austal, confirmou ter sido vítima de um ciberataque em dezembro de 2022, igualmente ligado a ransomware.

c. Setor Infraestruturas digitais

Os cabos submarinos são um elemento preponderante para a sociedade atual, pois:

"Subsea cables, are some of the most critical components of the global internet infrastructure. Estimates say that more than 97% of the world's internet traffic is transmitted via subsea cables. Subsea cables are therefore critical for the EU and protecting them from physical and cyber-attacks is strategically important59".

No presente caso, os 97% acima indicados referem-se ao tráfego entre continentes, por via marítima, onde alguns especialistas confirmam os 99%60. Os cabos submarinos são um elemento influente para a globalização, devido à interdependência crescente da sociedade, e que de forma simplificada a podemos caraterizar, no presente contexto, como um sistema mundial de comércio, finanças e comunicações instantâneo. Esta realidade baseia-se igualmente na existência do ciberespaço, que é uma criação humana, e em duas das suas três camadas: a camada física e a camada virtual61. Por sua vez, a Society for Worldwide Interbank Financial Telecommunication (SWIFT) depende totalmente de cabos submarinos, tendo em dezembro de 2022 registado uma média de 44,8 milhões de mensagens por dia, cujo tráfego cresceu +6,6% face ao ano anterior62. Os cabos submarinos são assim a espinha dorsal da economia global, com cerca de 10 biliões de dólares em transações financeiras transmitidas diariamente através destes cabos63. Como tal, pode afirmar-se que muitas destas características incluem componentes internacionais diversificados e altamente integrados, acrescentando complexidade e consequentemente aumentando os níveis de ameaça e gestão de risco.

A arquitetura de uma rede de uma infraestrutura de cabos submarinos assenta em três domínios: (1) no mar (Wet Plant), onde os cabos estão colocados para fazer a ligação entre estações; (2) em terra (Dry Plant), para a ligação à estação e entre estas e os respectivos Pontos de Presença/Centros para a ligação às redes terrestres; e (3) no ciberespaço, que é transversal aos dois anteriores e envolve os equipamentos, redes, sistemas e os cabos.

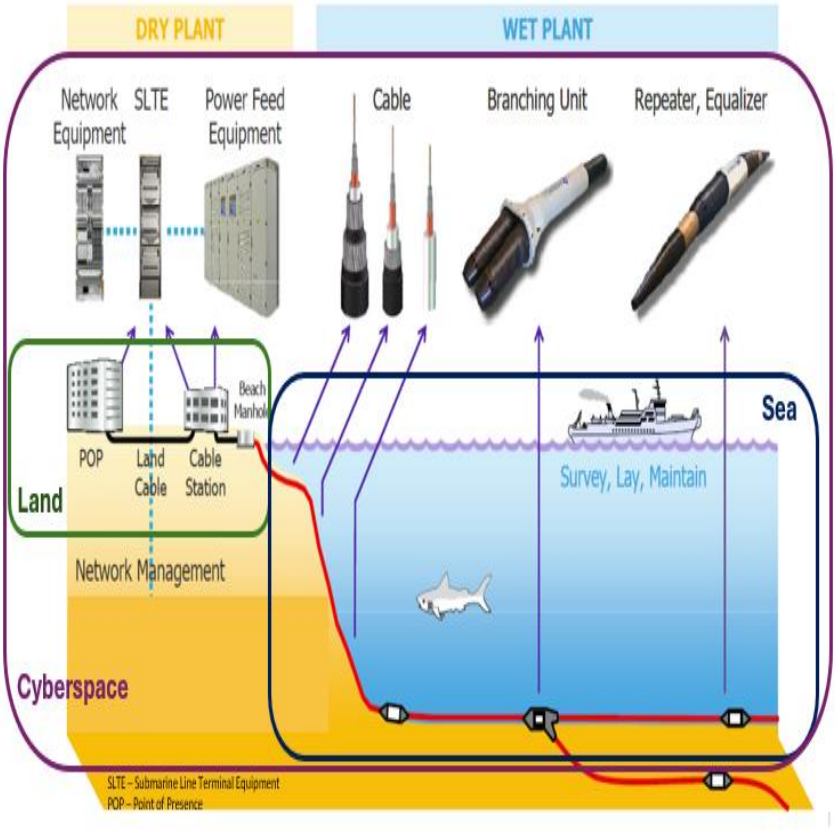

Imagem 1 – "High Speed Subsea Optical Networks"64, adaptado pelo autor.

Assim, a disrupção neste tipo de infraestruturas digitais pode ocorrer pela iniciativa de atores estatais ou não estatais e pode ser concretizada nestes três domínios. Ao contrário dos dois setores anteriores, apenas se apresentam exemplos de disrupções na infraestrutura física, por não haver muita informação deste tipo de ações com exclusividade no ciberespaço. No entanto, as disrupções com origem na dimensão física podem ter três origens: (1) Natural – devido a atividade na crosta terrestre, como sismos ou vulcões submarinos, podendo indicar-se o caso da interrupção no Mar Mediterrâneo em 2008, cuja causa terá decorrido de atividade sísmica registada perto de Malta. Jonathan Wright, director na Interoute, empresa que geria parte da rede de fibra óptica à altura do acontecimento, referiu que "Perderam três das quatro linhas, correspondendo a 90% do tráfego. Se o quarto cabo fosse interrompido, estar-se-ia perante um apagão total no Médio Oriente"65; ou a situação mais recente, em 2022, do vulcão Hunga Tonga-Hunga Ha'apai, no Tonga, que rompeu o único cabo de fibra ótica com 827 km de comprimento que liga Tonga ao resto do mundo66; (2) de atividade humana, podendo esta ser (a) acidental – devido a atividades de pesca, dragagens ou de se fundear em águas pouco profundas, perto da costa, constituindo-se este como o tipo mais comum67, correspondendo a cerca de 70% dos casos, num total anual de 150-200 incidentes68. Como um exemplo ilustrador indica-se a interrupção das telecomunicações nas ilhas Shetland, a 20 de outubro de 2022, provocada por um arrastão de pesca que atingiu o

principal cabo de telecomunicações entre a Escócia e estas ilhas[69]; ou (b) maliciosa – com duas vertentes: intenção de causar dano – onde o caso da deteção de três mergulhadores ao largo do porto de Alexandria pela Marinha Egípcia, em 2013, constitui-se como um bom exemplo, aquando da tentativa de cortarem um cabo submarino, o qual forneceria um terço de toda a capacidade de Internet entre a Europa e o Egipto[70]; ou para efeitos de espionagem – onde são necessários equipamentos especiais e apenas disponíveis em alguns Estados. Os submarinos especialmente equipados, ou submersíveis que operam a partir de navios como o Yantar russo, podem aceder a dados transmitidos nos cabos de fibra ótica sem causar danos, permitindo-lhes escutar, interromper e talvez modificar os dados transmitidos através destes cabos[71]. No entanto, não existem muitos dados sobre este tipo de incidentes, nem muitos relatos confirmados nos media. Por outro lado, o Comité Internacional de Proteção de Cabos (International Cable Protection Committee – ICPC) tem o registo de incidentes com cabos submarinos, e vários são de causa desconhecida[72]; (3) de origem animal – através de mordedura dos cabos, representando estas apenas 0,1% do total, o que é insignificante em comparação com outros tipos acima indicados, e que uma possível melhoria no design dos cabos poderia corrigir esta situação[73].

No caso de atividade maliciosa no ciberespaço, a preocupação estará naturalmente associada a evitar a disrupção nos sistemas que monitorizam a atividade dos cabos no fundo do oceano, que se encontram em centros de operações/segurança. Esta disrupção pode ser conseguida por ação interna (operador infiltrado ou descontente) ou externa (um hacker remoto). A interferência maliciosa com estes sistemas de monitorização essenciais poderá permitir que os atacantes ajustem alarmes, enganando assim os operadores com informação incorreta. O ataque à central nuclear de Natanz, no Irão, em 2010, com o malware Stuxnet [74], constitui-se como um bom exemplo, mas que implicou muitos recursos. Outra opção poderá ser através do engano dos operadores relativamente à localização de uma avaria, quando os tempos de reparação imediatos são essenciais para os milhões de clientes que dependem da disponibilidade destes cabos. Tendo em conta que a principal preocupação das empresas nesta área do negócio está associada aos lucros, alguns destes centros poderão ser construídos a baixo custo satisfazendo o limiar dos requisitos mínimos de segurança, o que também se constitui como uma preocupação. Por sua vez, embora seja inviável garantir a integridade e o funcionamento pleno dos cabos submarinos, existem medidas para salvaguardar tanto os cabos submarinos, como as estações associadas a estas infraestruturas, bem como os seus equipamentos, medidas estas que serão na dimensão física ou no contexto da cibersegurança.

4. Contexto Geopolítico – Cabos Submarinos

No contexto geopolítico, recentemente, verificaram-se atividades com impacto nos cabos submarinos, concretamente no Mar vermelho, com origem nas ações do grupo Houthi, do Iémen, um proxy do Irão. A 24 de fevereiro de 2024, três cabos submarinos que atravessam o Mar Vermelho foram danificados: o cabo Seacom/Tata, o Asia Africa

Europe-1 (AAE-1) e o Europe India Gateway (EIG), limitando a conectividade entre a Europa e a Ásia. Acredita-se que os cabos tenham sido cortados pela âncora do Rubymar, um cargueiro que foi atingido por um míssil[75], situação esta que coloca em perigo a segurança marítima nesta zona do globo. Pela sua relevância e impacto na economia europeia, esta ocorrência levou a que parlamento europeu elaborasse um documento sobre a temática[76]. Mas já em 2017, Rishi Sunak, então membro do parlamento do Reino Unido, publicou o relatório "Undersea Cables: Indispensable, insecure"[77], onde são levantadas diversas questões sobre esta problemática, nomeadamente:

"Whether from terrorist activity or an increasingly bellicose Russian naval presence, the threat of these vulnerabilities being exploited is growing. A successful attack would deal a crippling blow to Britain's security and prosperity. The threat is nothing short of existential. Working with global partners it is crucial that we act now to protect against these dangers, ensuring that our century's greatest innovation does not also become its undoing."

Associado a este tema, a NavalNews publicou o "5 Ways The Russian Navy Could Target Undersea Internet Cables" referindo que a Marinha Russa possui capacidades únicas de guerra submarina concebidas para operar em cabos submarinos[78].

De relevar também a disrupção sentida em 7-8 de outubro de 2023, no Mar Báltico, com danos extensos num gasoduto submarino e num cabo de comunicações que liga a Finlândia e a Estónia e cujas autoridades finlandesas referiram que "não poderiam ter ocorrido por acidente" e parecem ser o resultado de um "ato externo deliberado"[79]. Situação reforçada pelos presidente e primeiro-ministro da Finlândia, não querendo este especular sobre potenciais perpetradores antes de a investigação estar concluída, quando os media falavam em navios russos e chineses[80,81].

Pela pertinência deste assunto, a França apresentou em fevereiro de 2022 uma proposta de "Seabed Warfare Strategy"[82], pretendo assim proteger os interesses franceses e garantir a liberdade de ação das suas forças armadas, bem como aproveitar as oportunidades em apoio à sua autonomia estratégica, à semelhança do que foi feito para o ciberespaço e o espaço. Desta forma, tendo o presidente francês estabelecido os fundos marinhos como um dos dez objetivos estratégicos do roteiro "França 2030"[83], este documento constituiu-se como o compromisso do Ministério da Defesa.

Como nota final neste ponto, importa referir que historicamente, os cabos submarinos têm sido mantidos por consórcios de operadores de telecomunicações. Posteriormente, verificou-se a instalação de cabos submarinos por empresas para garantir uma maior largura de banda de Internet aos consumidores. Recentemente, verificou-se o interesse das Big Tech nesta área de negócio, nomeadamente a Google, a Meta (Facebook), a Microsoft e a Amazon que surgiram como investidores significativos em novos cabos, ultrapassando a capacidade implementada pelos operadores de Internet tendo em vista a tecnologia 5G[84]. Assim, como empresas de origem americana que são, facilmente se poderá inferir que serão um elemento a considerar na geopolítica do ciberespaço e mesmo na conflitualidade que ocorre neste domínio, onde o atual conflito entre a Rússia

e a Ucrânia assim o mostrou[85].

5. Terrorismo

Abordando a temática do terrorismo, e focalizando na dimensão digital dos oceanos, podemos recuar um pouco no tempo e lembrar Sherman Kent, um destacado dirigente da Agência Central de Informações (Central Intelligence Agency – CIA) no início da segunda metade do século XX, quando no seu livro "Strategic Intelligence for American World Policy"[86] refere que uma ameaça compreende dois elementos: a capacidade e a intenção. A "capacidade" como sendo a condição para um estado em atingir um determinado objetivo expressa em requisitos de tempo e força e "intenção" como sendo a definição dos seus objetivos e como pretende utilizar as suas capacidades para os alcançar. Entre Estados, como no tempo da guerra fria esta situação era compreensível, pois conheciam-se os adversários. No entanto, quando se transpõem estes conceitos para a ameaça terrorista, onde surgem atores não estatais, verifica-se uma alteração na análise. Isto porque pode assumir-se que a intenção estará sempre presente, ao passo que a existência de uma capacidade credível para atuar no ciberespaço já poderá ser discutível. Daí que para o tema neste documento, não existam registos significativos de grandes atentados no ciberespaço, tendo em vista uma disrupção significativa causando medo na população ou nos seus dirigentes.

A doutrina da Aliança Atlântica[87] estabelece que para as operações no ciberespaço, as ameaças neste domínio podem ser classificadas de acordo com a sua origem, tipo e técnica. No presente caso, de ameaças terroristas, a origem é intencional, o tipo poderá ser o comprometimento de funções decorrentes de subversão e as técnicas específicas de atividade maliciosa mais comuns são: (1) negação de serviço, para sobrecarga dos servidores; (2) deceção, levando os utilizadores autorizados a tomar ações que comprometam a segurança; (3) acesso não autorizado, para posterior escalada de privilégios para permitir ações adicionais; e (4) malware, instalado para disrupção ou exploração contínua do sistema.

Por sua vez, verifica-se que a atividade terrorista poderá concorrer cada vez mais para uma abordagem de maior diversidade e amplitude, no contexto das ameaças híbridas. Nesta análise, relembra-se uma obra de referência, concretamente o livro Conflict in the 21st Century: The Rise of Hybrid Wars, de Frank G Hoffman, onde ele apresenta a primeira definição de Hybrid Warfare[88] e refere que as ameaças híbridas incorporam uma gama completa de diferentes modos de guerra, incluindo capacidades convencionais, táticas irregulares, atos terroristas, onde se inclui a violência e coação indiscriminadas e a desordem criminal.

Face a uma possível natureza evolutiva das ameaças terroristas na Europa, o Conselho da Europa adotou uma estratégia antiterrorista para 2023-2027[89], oferecendo novas ferramentas e respostas concretas aos desafios contínuos e emergentes enfrentados pelas autoridades estatais. Esta estratégia assenta em três pilares, sendo eles a

Prevenção, a Acusação e a Proteção. No contexto do presente documento, alude-se à Prevenção, que se constitui pelas as medidas destinadas a impedir ataques terroristas ou à sua preparação através de medidas multifacetadas a longo prazo, e a Proteção de potenciais alvos de ataques terroristas, incluindo infraestruturas críticas, onde os cabos submarinos se constituem como um exemplo paradigmático.

Por sua vez, os diversos cortes que têm surgido com alguma regularidade nos cabos submarinos em África também têm limitado o combate ao terrorismo. Como exemplo, pode indicar-se o corte sentido em inícios de abril de 2024 na África Ocidental, que fez cair a conectividade em diversos países[90]. No caso da Nigéria, foi particularmente sentido na cidade de Maiduguri, capital do estado de Borno, o qual é o mais afectado pelo terror do Boko Haram e do seu grupo dissidente, o Estado Islâmico-África Ocidental. Com isto, as diversas organizações não governamentais (ONG) que aqui operam ficaram limitadas nos serviços prestados a apenas um terminal de satélite VSAT[91].

6. Considerações Finais

Para a presente reflexão, relativa à dimensão digital dos oceanos, incidiu-se a análise nas infraestruturas críticas, na medida em que estas se podem constituir como um alvo para atentados com fins terroristas. Consideraram-se os setores da energia, dos transportes e das infraestruturas digitais, onde a vertente económica se afigura como sendo plausível de poder ser adotada pelos terroristas, tendo por base o carácter assimétrico associado. As vulnerabilidades nestes setores, podem ser exploradas para diversos fins criminosos, seguindo uma mesma lógica, onde se insere o terrorismo ou o ransonware, entre outros. No que ao ciberespaço diz respeito, as atividades criminosas seguirão a metodologia da Cyber Kill Chain, pela sua aplicabilidade generalizada na caraterização da criação de efeitos perversos no ciberespaço. Relativamente à utilização do ciberespaço para ações terroristas no contexto da presente reflexão, apesar das poucas evidências conhecidas, assiste-se muitas vezes a uma valorização destas ações, pela dimensão dos seus possíveis impactos.

Com uma abordagem holística, os exemplos referidos mostraram as disrupções na dimensão física e no ciberespaço, tendo em vista reforçar a interdependência e a complexidade que hoje se vive. Assim, relevaram-se os cabos submarinos no contexto das infraestruturas digitais, pela dependência que a sociedade atual tem destes sistemas, onde as ações maliciosas que se verificaram no Mar Vermelho em 2013, ou mais recentemente, em 2023, no Mar Báltico se podem constituir como exemplo. Por sua vez, a sabotagem do gasoduto Nord Stream veio mostrar que o ataque a infraestruturas críticas para fins militares já não está confinado aos limites geográficos de uma zona de conflito, exponenciando a superfície de ataque de forma muito significativa. Esta situação é facilmente extensível aos cabos submarinos, a qual é passível de ser explorada por atores estatais e não estatais, vendo nestes sistemas uma forma de limitar a ação dos Estados, o que constitui uma preocupação para a nossa sociedade.

Desta forma, pode concluir-se que tais incidentes, de forma deliberada, exemplificam como as infraestruturas críticas se tornaram um instrumento da guerra contemporânea, onde os conflitos são cada vez mais híbridos e os setores críticos passam a ser armas da guerra moderna, onde o terrorismo será sempre uma ameaça a considerar.

---

* Este artigo foi elaborado no contexto da 7.ª Conferência Internacional sobre Terrorismo Contemporâneo, subordinada ao tema das "Novas Ameaças Emergentes", realizada no ISCSP, em 16 de maio de 2024.

1 Bruce Hoffman, ex-diretor da RAND, define terrorismo como "the deliberate creation and exploitation of fear through violence or the threat of violence in pursuit of political change." Bruce Hoffman, Inside Terrorism (New York: Columbia University Press, 1998). Disponível em https://archive.nytimes.com/www.nytimes.com/books/first/h/hoffman-terrorism.html

2 Preparing for the Psychological Consequences of Terrorism: A Public Health Strategy. Stith Butler A, Panzer AM, Goldfrank LR, editors, 2003.Institute of Medicine (US) Committee on Responding to the Psychological Consequences of Terrorism, Washington (DC): National Academies Press (US); 2003. Disponível em https://www.ncbi.nlm.nih.gov/books/NBK221638/#ddd00037

3 Disrupção – 'termo inglês "disruption" traduz-se em português como perturbação (ver The Oxford Paperback Portuguese Dictionary), sendo cada vez mais frequente a ocorrência desta palavra com o sentido que lhe é atribuído em inglês, o de "perturbação". Disponível em https://ciberduvidas.iscte-iul.pt/consultorio/perguntas/disrupcao/14349

4 Ciberataque – Um ciberataque é uma tentativa de cibercriminosos, hackers ou outros adversários digitais de acederem a uma rede ou sistema informático, geralmente com o propósito de alterar, roubar, destruir ou expor informação. Disponível em https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

5 Cyber Kill Chain, Lockheed Martin. Disponível em https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

6 Defending Against Cyber Attacks: A Lockheed Martin Overview. Disponivel em https://www.youtube.com/watch?v=4Vz_uP0I-x4&t=66s

7 What is Interpol. Dispponível em https://www.interpol.int/Who-we-are/What-is-INTERPOL; 6 Facts About How Interpol Fights Cybercrime. Ericka Chickowski, May 27, 2024, Darkreading. Disponível em https://www.darkreading.com/cyberattacks-data-breaches/5-facts-about-how-interpol-fights-cybercrime

8 A União Europeia considera a segurança do ciberespaço como "Cybersecurity", numa visão mais holística da sua proteção e segurança, aplicando este mesmo termo para as questões mais técnicas.

9 Cyber Diplomacy Toolkit Links. Disponível em https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy_Links.html

10 Cibersegurança – consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem. Ref: Estratégia Nacional de Segurança do Ciberespaço 2019-2023. https://www.cncs.gov.pt/pt/estrategia-nacional/

11 Ao longo deste documento serão utilizados os termos diretiva NIS2 e diretiva CER, por uma maior facilidade de ligação entre o termo em inglês e a sua aplicação em português.

12 Estratégia de cibersegurança da UE para a década digital. Disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A52020JC0018

13 Diretiva NIS, ANACOM, 24.08.2016. Disponível em https://www.anacom.pt/render.jsp?contentId=1393965

14 Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555

15 Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), European Commission. Disponível em https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

16 Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção.

17 Directive on the Resilience of Critical Entities. 2021Portugal.eu. Disponível em https://www.consilium.europa.eu/media/48760/resilience-of-critical-entities-directive.pdf#:~:text=The%20Portuguese%20Presidency%20Work%20Programme%20for%20the,priority%20%22Strengthening%20the%20

resilience%20of%20our%20societies%22.&text=This%20instrument%20aims%20to%20contribute%20to%20strengthening,the%20good%20functioning%20of%20the%20internal%20market

18 Resiliência da UE: Conselho adota diretiva destinada a reforçar a resiliência das entidades críticas, Conselho da UE, 8 dezembro 2022, Comunicado de imprensa. Disponível em https://www.consilium.europa.eu/pt/press/press-releases/2022/12/08/eu-resilience-council-adopts-a-directive-to-strengthen-the-resilience-of-critical-entities/

19 Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2557

20 Critical Entities Resilience Directive (CER) | Updates, Compliance. Disponível em https://www.critical-entities-resilience-directive.com/

21 Critical infrastructure Resilience, European Commission, 24 July 2024. Disponível em https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en

22 The Most Consequential Act of Sabotage in Modern Times. Mark Bowden, December 13, 2023, The Atlantic. Disponível em https://www.theatlantic.com/international/archive/2023/12/nord-stream-pipeline-attack-theories-suspects-investigation/676320/

23 Statement by the North Atlantic Council on the damage to gas pipelines. Disponível em https://www.nato.int/cps/en/natohq/official_texts_207733.htm

24 Seabed warfare: Protecting the UK's undersea infrastructure. Uk Parliament, House of Commons Library, 24 May, 2023. Disponível em

https://commonslibrary.parliament.uk/seabed-warfare-protecting-the-uks-undersea-infrastructure/

25 Protection of Undersea Telecommunication Cables: Issues for Congress, Congressional Research Service. August 7, 2023. Disponível em https://sgp.fas.org/crs/misc/R47648.pdf

26 'Nord Stream' – the need to prioritise security of critical infrastructure at sea, Meredith Primrose Jones & Aiden Warren, 05 October 2022, RMIT University. Disponível em https://www.rmit.edu.au/news/ccsri/nord-stream-critical-sea-infrastructure

27 Recomendação do Conselho sobre um plano de ação para a coordenação da resposta a nível da UE a perturbações em infraestruturas críticas com importante relevância transfronteiriça Bruxelas, 6.9.2023 / COM(2023) 526 final / 2023/0318(NLE). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52023DC0526

28 Vilnius Summit Communiqué. NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius, 11 July 2023. Disponível em https://www.nato.int/cps/en/natohq/official_texts_217320.htm

29 Washington Summit Declaration, NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, 10 July 2024. Disponível em https://www.nato.int/cps/en/natohq/official_texts_227678.htm

30 Ukrainian military officer coordinated Nord Stream pipeline attack, Shane Harris e Isabelle Khurshudyan, November 11, 2023, The Washington Post. Disponível em https://www.washingtonpost.com/national-security/2023/11/11/nordstream-bombing-ukraine-chervinsky/

31 All the Evidence Points To Kyiv, Spiegel international, 26.08.2023. Disponível em https://www.spiegel.de/international/europe/investigating-the-attack-on-nord-stream-all-the-clues-point-toward-kyiv-a-124838c7-992a-4d0e-9894-942d4a665778

32 Nord Stream sabotage: Germany issues arrest warrant, Deutsche Welle, 14.08.2024. Disponível em https://www.dw.com/en/nord-stream-explosions-germany-issues-arrest-warrant/a-69933920

33 Security Council Rejects Draft Resolution Establishing Commission to Investigate

Sabotage of Nord Stream Pipeline, United Nations, 27 March 2023. Disponível em https://press.un.org/en/2023/sc15243.doc.htm

34 Part 4. Turkey's geopolitical role in the Black Sea and European energy security: From pipelines to liquefied natural gas. Eser Özdil, September 13, 2024, Atlantic Council. Disponível em https://www.atlanticcouncil.org/in-depth-research-reports/report/part-4-turkeys-geopolitical-role-in-the-black-sea-and-european-energy-security-from-pipelines-to-liquefied-natural-gas/

35 EU Energy Platform: Facilitating joint purchases of gas. Briefing, 11-07-2023. Disponível em https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)751411

36 The end of Nord Stream 2- Germany, The United States, and EU Law. Alan Riley, 2022, Atlantic Council. Disponível em https://huri.harvard.edu/files/huri/files/ns2_report_3_riley.pdf?m=1647643174

37 Permanent Rupture: The European-Russian Energy Relationship Has Ended with Nord Stream. Emily Holland, October 3, 2022, War on the rocks. Disponível em https://warontherocks.com/2022/10/permanent-rupture-the-european-russian-energy-relationship-has-ended-with-nord-stream/

38 If Russia invades Ukraine, there will be no Nord Stream 2, Biden says, Reuters, February 8, 2022. Disponível em https://www.reuters.com/business/energy/if-russia-invades-ukraine-there-will-be-no-nord-stream-2-biden-says-2022-02-07/

39 President Biden on Nord Stream 2 Pipeline if Russia Invades Ukraine: "We will bring an end to it." Disponível em https://www.youtube.com/watch?v=OS4O8rGRLf8

40 Shamoon (2012), CCDCOE, disponível em https://cyberlaw.ccdcoe.org/wiki/Shamoon_(2012)

41 The Cyber Attack on Saudi Aramco, Christopher Bronk and Eneken Tikk-Ringas, April-May 2013, pp. 81-96, Survival, vol. 55 no. 2, DOI 10.1080/00396338.2013.784468. Disponível em https://www.researchgate.net/publication/263449655_The_Cyber_Attack_on_Saudi_Aramco

42 Shipping and World Trade: World Seaborne Trade. Disponível em https://www.ics-shipping.org/shipping-fact/shipping-and-world-trade-world-seaborne-trade/

43 Maritime traffic definition, Law Insider. Disponível em https://www.lawinsider.com/dictionary/maritime-traffic

44 Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States, Joseph R. Biden Jr., White House, February 21, 2024. Disponível em https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/21/executive-order-on-amending-regulations-relating-to-the-safeguarding-of-vessels-harbors-ports-and-waterfront-facilities-of-the-united-states/

45 White House, U.S. Coast Guard Seek to Address Maritime Cyber Espionage and Cybersecurity Risks. Sean T. Pribyl, Shardul Desai, Jameson B. Rice, March 19, 2024, Holland & Knight Alert. Disponível em https://www.hklaw.com/en/insights/publications/2024/03/white-house-us-coast-guard-seek-to-address-maritime

46 Suez blockage is holding up $9.6bn of goods a day, Justin Harper, BBC, 26 March 2021. Disponível em https://www.bbc.com/news/business-56533250

47 Eilat Port to lay off half its staff due to Houthi attacks stymieing shipping trade, Times of Israel Staff, 20 March 2024. Disponível em https://www.timesofisrael.com/eilat-port-to-lay-off-half-its-staff-due-to-houthi-attacks-stymieing-shipping-trade/

48 Maritime cyber security: Piecing the puzzle together, Safety4sea-The editorial team, June 27, 2024. Disponível em https://safety4sea.com/maritime-cyber-security-piecing-the-puzzle-together/

49 Preventing Catastrophic Cyber–Physical Attacks on the Global Maritime Transportation System: A Case Study of Hybrid Maritime Security in the Straits of Malacca and Singapore, Adam James Fenton, 19 March 2024, Journal of Marine Science and Engineering. Disponível em https://www.mdpi.com/2077-1312/12/3/510

50 A Retrospective Analysis of Maritime Cyber Security Incidents, Per Håkon Meland, Karin Bernsmed, Egil Wille, Ørnulf Jan Rødseth, Dag Atle Nesheim, January 2021, TransNav the International Journal on Marine Navigation and Safety of Sea

Transportation, DOI:10.12716/1001.15.03.04. Disponível em https://www.researchgate.net/publication/354657671_A_Retrospective_Analysis_of_

Maritime_Cyber_Security_Incidents

51 Ransomware – "um tipo de software malicioso, ou malware, que ameaça uma vítima ao destruir ou bloquear o acesso a dados ou sistemas críticos até que um resgate seja pago". Disponível em https://www.microsoft.com/pt-pt/security/business/security-101/what-is-ransomware

52 Ataque DDOS – efetua-se através do envio de múltiplas solicitações para o recurso Web invadido com o objetivo de exceder a capacidade que o site tem de lidar com diversas solicitações, impedindo seu funcionamento correto (https://www.kaspersky.com.br/resource-center/threats/ddos-attacks).

53 Malware – termo genérico para qualquer tipo de software malicioso concebido para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável (https://www.mcafee.com/pt-pt/antivirus/malware.html).

54 Viking Line in Crisis: Cyberattack Paralyzes Shipping Industry Across Europe, Editorial, The Cyber Express, October 20, 2023. Disponível em https://thecyberexpress.com/viking-line-cyberattack-europe-shipping-indust/

55 Chinese Spy Malware Found in European Shipping Companies' Systems, The Maritime Executive, May 15, 2024. Disponível em https://maritime-executive.com/article/chinese-spy-malware-found-in-european-shipping-companies-systems

56 Ransomware attack on maritime software impacts 1,000 ships, Jonathan Greig, January 17th, 2023, The Record. Disponível em https://therecord.media/ransomware-attack-on-maritime-software-impacts-1000-ships

57 Comunicado, Porto de Lisboa, 26 de dezembro de 2022. Disponível em https://www.portodelisboa.pt/pt/-/press-release

58 Ransomware attack on US Navy shipbuilder leaked information of nearly 17,000 people, Jonathan Greig, January 12th, 2024, The Record. Disponível em https://therecord.media/fincantieri-shipbuilder-us-navy-wisconsin-ransomware

59 Undersea cables – What is at Stake?, ENISA, August 31, 2023. Disponível em https://www.enisa.europa.eu/publications/undersea-cables

60 Do Submarine Cables Account For Over 99% of Intercontinental Data Traffic?, Alan Mauldin May 4, 2023. Disponível em https://blog.telegeography.com/2023-mythbusting-part-3

61 JP 3-12, Joint Cyberspace Operations, 8 June 2018. Disponível em https://irp.fas.org/doddir/dod/jp3_12.pdf. Já existe uma nova edição, publicada em 2022, mas que não está disponível ao público. No entanto, este conceito de três camadas mantém-se

62 Swift FIN Traffic & Figures. Disponível em https://www.swift.com/pt/node/3831

63 Security threats to undersea communications cables and infrastructure – consequences for the EU, Christian BUEGER, Tobias LIEBETRAU, Jonas FRANKEN, June 2022, European Parliament. Disponível em https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

64 "High Speed Subsea Optical Networks", Telxius, CHI-NOG, May 10, 2018, disponível em https://x.com/ogawa_tter/status/1340093022550122497/photo/3

65 Asia and Mideast Internet disrupted by cut cable, Joshua Keating, December 19, 2008, Foreign Policy. Disponível em https://foreignpolicy.com/2008/12/19/asia-and-mideast-internet-disrupted-by-cut-cable/

66 Tonga Calamity: Impact of Natural Disasters on Submarine Cables, Krutika Patil, February 01, 2022, Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA). Disponível em https://www.idsa.in/idsacomments/tonga-calamity-kpatil-010222#footnote11_ba60dmd

67 How is subsea cable repaired?, Sarah Whiteford, Apr 23, 2021, Disponível em https://www.onesteppower.com/post/subsea-cable-repair

68 Strategic importance of, and dependence on undersea cables, Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2019. Disponível em https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf

69 UK-registered fishing vessel damaged Shetland subsea cable, Oliver McBride, Dec 8, 2022, Irish, Scottish & UK Fishing News. Disponível em https://thefishingdaily.com/latest-news/uk-registered-fishing-vessels-damaged-shetland-subsea-cable/

70 Undersea internet cables off Egypt disrupted as navy arrests three, Charles Arthur, 28 Mar 2013, The Guardian. Disponível em https://www.theguardian.com/technology/2013/mar/28/egypt-undersea-cable-arrests

71 Strategic importance of, and dependence on undersea cables, CCDCOE, 2019.

72 Undersea cables – What is at Stake?, ENISA, 2023.

73 Submarine Cable Protection and the Environment, Mike Clare, March 2021, International Cable Protection Committee (ICPC). Disponível em https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf

74 Hacking Industrial Control Systems, Eric D. Knapp e Joel Thomas Langill, 2015, Industrial Network Security (Second Edition). Disponível em https://www.sciencedirect.com/topics/computer-science/stuxnet

75 East African Internet connectivity again impacted by submarine cable cuts, David Belson, 2024-05-13, cloudflare. Disponível em https://blog.cloudflare.com/east-african-internet-connectivity-again-impacted-by-submarine-cable-cuts/

76 Recent threats in the Red Sea Economic impact on the region and on the EU, European Parliament, 2024. Disponível em https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760390/EPRS_BRI(2024)760390_EN.pdf

77 Undersea Cables: Indispensable, insecure, Rishi Sunak, 2017, Policy Exchange. https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/

78 5 Ways The Russian Navy Could Target Undersea Internet Cables, H. Suttom, 07 April 2021. Disponível em https://www.navalnews.com/naval-news/2021/04/5-ways-the-russian-navy-could-target-undersea-internet-cables/

79 Undersea pipeline damage appears to be deliberate, says Finland, Jon Henley, 10 Oct 2023, The Guardian. Disponível em https://www.theguardian.com/world/2023/oct/10/undersea-pipeline-damage-appears-to-be-deliberate-says-finland

80 Estonia focuses on Chinese vessel in investigation into underwater cable damage, Andrius Sytas, October 25, 2023, Reuters. Disponível em https://www.reuters.com/world/europe/estonia-focuses-chinese-vessel-investigation-into-underwater-cable-damage-2023-10-25/

81 Who is sabotaging underwater infrastructure in the Baltic Sea?, The Economist, Oct 22, 2023. Disponível em https://www.economist.com/europe/2023/10/22/who-is-sabotaging-underwater-infrastructure-in-the-baltic-sea

82 Seabed Warfare Strategy, Ministère des Armées, February 2022. Disponível em https://www.archives.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf

83 France 2030: Bringing the future closer, Business France. Disponível em https://investinfrance.fr/wp-content/uploads/2017/08/Le-France-2030-Digest-version-anglaise-janvier-2023.pdf

84 Strategic importance of, and dependence on undersea cables, CCDCOE, 2019.

85 International support to Ukraine in cyberspace in the Ukraine Russia conflict, Helder Fialho Jesus, April 2024, Military Operations in Cyberspace Conference, 06May2023, Lisbon, Military University Institute. Disponível em https://www.ium.pt/pub/190

86 Strategic Intelligence For American World Policy, Sherman Kent, 1965, Archon Books Hamden, Connecticut. Disponível em https://archive.org/details/in.ernet.dli.2015.86810/page/n5/mode/2up?q=Intentions

87 Allied Joint Doctrine for Cyberspace Operations, AJP-3.20, 2020. Disponível em https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

88 Hybrid Warfare, John G.L.J. Jacobs, Martijn W.M. Kitzen, 22 September 2021, DOI:

10.1093/obo/9780199743292-0260. Disponível em https://www.oxfordbibliographies.com/display/document/obo-9780199743292/obo-9780199743292-0260.xml

89 Council of Europe adopts new counter-terrorism strategy for 2023-2027, Council of Europe, 8 February 2023. Disponível em https://www.coe.int/en/web/portal/-/council-of-europe-adopts-new-counter-terrorism-strategy-for-2023-2027

90 2024 West Africa Submarine Cable Outage Report, Internet Society, April 2024. Disponível em https://www.internetsociety.org/wp-content/uploads/2024/04/2024-West-Africa-Submarine-Cable-Outage-Report.pdf

91 Undersea Cable Cuts Hinder Nigeria Fight Against Terrorism, Emeka Okonkwo, April 5, 2024, CAJ News Africa. Disponível em https://subtelforum.com/undersea-cable-cuts-impact-nigeria-terrorism-fight/