EuroDefense Portugal

NEWSLETTER

NÚMERO 22 | DEZ 2022

SOBERANIA DIGITAL

Desafio Europeu para uma Autonomia Estratégica Tecnológica

Sumário Executivo

O conceito de Soberania Digital surgiu recentemente como resultado da crescente importância e dependência das nossas sociedades na tecnologia, e das preocupações dos Estados em promover a autonomia estratégica no domínio digital. Este artigo pretende demonstrar como a Soberania Digital é fundamental no mundo atual, e na Europa em particular, para garantir a nossa segurança, conforto e prosperidade, preservando valores compartilhados que conquistamos ao longo da nossa história. Para atingir este objetivo, começa por introduzir um quadro de referência para o poder cibernético e os cenários onde ele é, e pode ser, aplicado. De seguida é realizada uma análise dos pontos de confluência no ciberespaço, através das camadas cognitivas, informativas e físicas deste domínio, identificando vulnerabilidades onde o poder cibernético pode ser alavancado. Este trabalho finaliza almejado para uma visão geral do que a Europa está, e pode fazer, para manter a sua autonomia estratégica tecnológica, dando enfoque à resiliência.

Contexto

A soberania, em teoria política, é o supervisor final, ou autoridade, no processo decisório do Estado e na manutenção da ordem. Podemos também encontrar outras definições relacionadas com população, território, governo e independência.

No mundo atual, cada vez mais dependente da tecnologia, o conceito de território atravessa as fronteiras tradicionais que normalmente conhecemos, para o ciberespaço, para onde se deslocam a maioria das atividades e serviços essenciais da sociedade. A manutenção da autoridade, ordem, ou tomada de decisões independentes neste domínio, exige que os governos controlem a forma como a tecnologia é utilizada para apoiar as nossas vidas, como cidadãos, numa sociedade democrática.

Existe uma preocupação crescente, e baseada em fatos, de que nós, europeus, estamos gradualmente a perder o controle sobre os nossos dados, a nossa capacidade de inovar ou a nossa capacidade de proteger infraestruturas críticas e operação de serviços essenciais. As gigantes tecnológicas são, maioritariamente, dos EUA e da China, e gerem serviços de computação em nuvem para todo o mundo, mas também fabricam os servidores e equipamentos de comunicações que utilizamos nas nossas empresas, nas nossas casas, ou nos nossos serviços institucionais. Mesmo tendo a consciência de que um número relevante desses fornecedores e adquiridos de serviços estão baseados em países amigos, com os quais compartilhamos valores, não ter a capacidade de agir independentemente no mundo digital, pode representar um risco a curto e longo prazo para a nossa sociedade europeu.

Desta forma, a capacidade da Europa para agir de forma independente no mundo digital, moldando e impondo legislação no seu ambiente, é uma discussão urgente, perante uma compreensão profunda do desafio, um acompanhamento contínuo da situação, bem como ações a curto e longo prazo para superar os riscos.

Paulo Moniz
EuroDefense-Portugal

Novas tecnologias trazem novos riscos, e o impacto de ataques cibernéticos por meio de produtos digitais aumentou drasticamente nos últimos anos. Cada vez mais, os consumidores são vítimas de falhas de segurança ligadas a produtos digitais, como intercomunicadores para bebé, aspiradores robóticos, roteadores Wi-Fi e sistemas de alarme. Para as empresas, a importância de garantir que os produtos digitais na cadeia de suprimentos sejam seguros tornou-se fundamental, considerando que três em cada cinco fornecedores já perderam dinheiro devido a falhas de segurança do produto. A proposta de regulamento da Comissão Europeia, o *'cyber-resilience act'* visa, portanto, impor obrigações de cibersegurança a todos os produtos com elementos digitais cujo uso pretendido e previsível inclua ligação direta ou indireta de dados a um dispositivo ou rede. A proposta introduz princípios de cibersegurança desde a conceção e por defeito impõe um dever de zelar pelo ciclo de vida dos produtos.

A invasão não provocada da Rússia na Ucrânia coloca a necessidade de resiliência europeia em foco mais nítida e defende um novo enquadramento da abordagem da resiliência da NATO. Embora a resiliência seja principalmente uma responsabilidade nacional que requer compromisso político, investimento, políticas e instituições de apoio e priorização, há um forte argumento para que a resiliência se torne um imperativo coletivo, bem como doméstico. A resiliência deve ser reconceituada como a capacidade individual e coletiva de resistir, lutar e recuperar-se rapidamente de perturbações causadas por ameaças militares e não militares à segurança euro-atlântica de atores autoritários e concorrentes estratégicos, bem como desafios globais. Merece uma prioridade máxima na NATO e no planeamento nacional, um investimento significativo na construção de uma postura de resiliência credível da Europa e novas abordagens para ampliar a capacidade combinada dos aliados para enfrentar desafios e ameaças comuns, bem como aumentar a vigilância no meio de tensões elevadas.

Interferência de manipulação de informações estrangeiras e segurança cibernética

A Agência da UE para a Cibersegurança (ENISA) e o Serviço Europeu de Ação Externa (EEAS) uniram forças para estudar e analisar o cenário de ameaças relacionadas à Manipulação e Interferência de Informações Estrangeiras (FIMI) e à desinformação. É apresentado um quadro analítico dedicado, consistente com a metodologia ENISA *Threat Landscape*, com o objetivo de analisar os aspetos FIMI e de cibersegurança da desinformação. O conceito de FIMI foi proposto pelo EEAS, como uma resposta ao apelo do Plano de Ação para a Democracia Europeia para um maior refinamento das definições em torno da desinformação. Embora a desinformação seja uma parte proeminente do FIMI, o FIMI enfatiza o comportamento manipulador, em oposição à veracidade do conteúdo entregue.
Os documentos estratégicos (*Strategic Compass for Security and Defense* e as Conclusões do Conselho), referem-se à importância de combater o FIMI, bem como as ameaças híbridas e cibernéticas.

"Inteligência Artificial" (IA) é um termo coletivo que denota um conjunto de tecnologias que permitem aos computadores colher informações a partir de dados e, dependendo da situação, agir sobre essas informações iniciando o processamento adicional de dados ou causando eventos no mundo físico. A "Inteligência Artificial" está sendo amplamente discutida nos últimos anos, tanto globalmente quanto na União Europeia. Nesse discurso, foi levantada uma forte expressão tanto das grandes oportunidades de desenvolvimento da IA quanto das múltiplas ameaças para as pessoas, especialmente no que diz respeito às profissões em que robots e IA substituiriam os humanos. A IA pode colocar nossas vidas privadas sob vigilância permanente e, eventualmente, podemos perder o controle sobre as tecnologias. É essencial superar essas ameaças e abrir caminho para a construção da IA confiável. Em tempos de pandemia, não apenas a conscientização sobre possíveis oportunidades de IA aumentou enormemente, mas também a digitalização se acelerou.

A invasão russa da Ucrânia, embora principalmente uma guerra cinética, viu novos atores e novas atividades explorando o ciberespaço. Numerosos atores não estatais, grupos de hackers e empresas comerciais entraram no campo de batalha virtual, tomando partido de um dos estados em guerra sem necessariamente serem entidades beligerantes. Enquanto os estados já estavam lutando para regular as atividades no ciberespaço, os novos tropos, técnicas e táticas aumentaram a incerteza jurídica. O direito internacional é baseado no estado, no território e na distinção entre guerra e paz, enquanto o ciberespaço e as atividades nele conduzidas não são. A guerra russo-ucraniana deixou claro que atores não estatais como a *Microsoft* ou o *Anonymous* não podem ser atribuídos a um estado e que eles não participam diretamente das hostilidades, pelo menos não fisicamente. Além disso, os atributos do ciberespaço não apenas obscureceram as diferenças entre atores estatais e não estatais, mas também transformaram a dicotomia entre guerra e paz.

FORTALECIMENTO DA RESILIÊNCIA CIBERNÉTICA

Ver mais

A presente avaliação de impacto (AI) acompanha a proposta de requisitos horizontais de cibersegurança para produtos com elementos digitais. Os pontos fortes da AI incluem uma definição bem fundamentada do problema, uma base de evidências que parece ser recente e relevante e um relato transparente das suposições e limitações da análise. Além disso, foi feito um esforço na AI para quantificar os custos e benefícios totais para os fabricantes de produtos com elementos digitais.

ESCOLHAS DIFÍCEIS NUM ATAQUE DE RANSOMWARE

Ver mais

Os ataques de ransomware começaram como uma novidade, mas agora tornaram-se um perigo claro e presente para entidades de todos os tamanhos e funções. O número de ataques de ransomware e o preço dos resgates exigidos aumentaram vertiginosamente desde 2018. A legislação e as políticas não acompanharam. Os formuladores de políticas têm procurado moldar a estrutura de incentivos para que as vítimas incentivem a defesa e desincentivem o pagamento de resgates.

PODER DE SOFTWARE

Ver mais

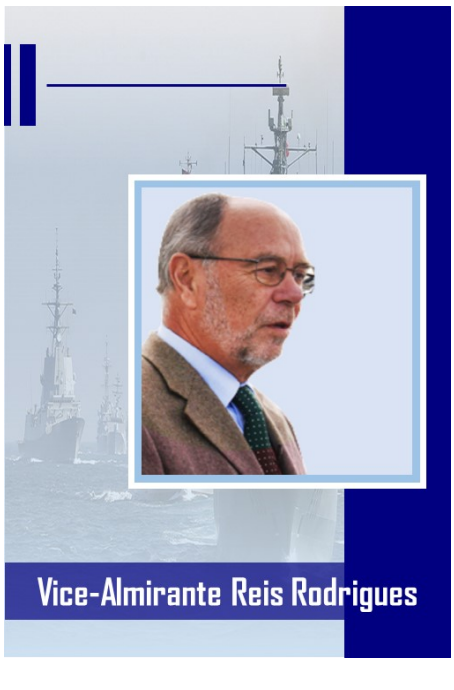
As implicações económicas e geopolíticas

O código aberto desempenha um papel central no desenvolvimento de software, tanto em paralelo com o software proprietário quanto cada vez mais interligado com ele. Tornou-se um fator importante para os processos de inovação das empresas e para o sucesso e popularidade dos seus produtos. Para os utilizadores, o uso de software de código aberto pode aliviar os riscos decorrentes de soluções proprietárias, incluindo questões de privacidade de dados ou restrições comerciais.

CENÁRIO DE AMEAÇAS ENISA 2022

Ver mais

Os ataques de cibersegurança continuaram a aumentar durante o segundo semestre de 2021 e 2022, não apenas em termos de vetores e números, mas também em termos de impacto. A crise Rússia-Ucrânia definiu uma nova era para a guerra cibernética e o hacktivismo, o seu papel e o impacto nos conflitos. É muito provável que os Estados e outras operações cibernéticas se adaptem a este novo estado de coisas e aproveitem as novidades e desafios trazidos por esta guerra. No entanto, esse novo paradigma trazido pela guerra tem implicações para as normas internacionais no ciberespaço.



Vice-Almirante Reis Rodrigues

É com muito pesar que noticiamos o falecimento do Vice-Almirante Alexandre Reis Rodrigues, no passado dia 15 de dezembro.

A sua brilhante carreira militar ficou assinalada pelo exercício de relevantes funções e o acesso aos mais altos postos de comando na Marinha portuguesa e em estruturas europeias (UEO) e da NATO, designadamente, como Vice-Chefe do Estado Maior da Armada, Comandante do Quartel-General da NATO em Oeiras, comandante da EUROMARFOR. Em 1995, foi-lhe confiada a missão de comandar a STANAVFORTLAND, a mais antiga e prestigiada força operacional permanente da NATO, utilizada nessa altura em operações de manutenção da paz na região dos Balcãs. Era a primeira vez que o nosso País assumia tão importante tarefa no quadro da Aliança Atlântica.

Já na situação de reserva, escreveu diversos livros e artigos dedicados às áreas da Segurança, da Defesa e dos assuntos militares, tendo sempre em vista contribuir para o aprofundamento do conhecimento e da sensibilização da sociedade civil para as questões de defesa nacional e europeia. Com este mesmo propósito, fundou o jornal digital “Defesa e Relações Internacionais”, onde se encontram reflexões independentes e opiniões muito construtivas sobre os assuntos mais relevantes da política de defesa nacional, das forças armadas e da segurança internacional.

A Direção do Centro de Estudos EuroDefense-Portugal recorda que o Vice-Almirante Reis Rodrigues foi membro ativo do Conselho Consultivo e um Amigo da EuroDefense desde a sua fundação e, por isso, lhe prestamos a nossa sentida homenagem e público reconhecimento pelo seu inestimável contributo para o prestígio desta organização.

À sua Família apresentamos as nossas sentidas condolências.

Os europeus devem lidar com o mundo como ele é, não como eles gostariam que fosse. E isso significa reaprender a linguagem do poder e combinar os recursos da União Europeia de forma a maximizar o seu impacto geopolítico. ***Josep Borrell***

Uma sociedade digital próspera não pode existir sem uma postura de defesa cibernética que atenda adequadamente aos desafios impostos pela nossa dependência de tecnologia e plataformas baseadas na Internet. Mas o ciberespaço aberto e global que promove o crescimento económico e ajuda a tirar milhões de pessoas da pobreza é, ao mesmo tempo, uma fonte de vulnerabilidade para as sociedades europeias. Em tempos de paz, atores estatais e não estatais recorrem a operações no ciberespaço para interromper o bom funcionamento das sociedades democráticas, minar governos legítimos, recolher inteligência e roubar segredos comerciais ou dinheiro. Operações cibernéticas contra alvos europeus conduzidas por procuradores estatais e grupos criminosos que operam na China, Rússia, Coreia do Norte e Irão prejudicam seriamente a competitividade europeia e o nosso tecido social.

A dimensão cibernética da guerra Rússia-Ucrânia foi extensa. Ela revela as características do conflito cibernético moderno entre Estados bem combinados. Embora a sua componente predominante tenha sido uma batalha massiva de "informação" online por corações e mentes, ampliada de forma compreensível por indivíduos e grupos privados de cibervigilantes, também envolveu uma grande e concertada campanha russa para interromper a infraestrutura crítica ucraniana. Isso foi amplamente atenuado pela solidez da segurança cibernética ucraniana, reforçada pela assistência ocidental.

No entanto, permanece o risco de que o conflito cibernético possa escalar além do ciberespaço para um confronto mais amplo entre a Rússia e a NATO. As chances de isso acontecer são aumentadas pela incerteza sobre a verdadeira natureza das operações cibernéticas, o seu uso responsável e, especialmente, como o direito internacional se aplica a elas, tornando os esforços dos Estados para lidar com essas questões urgentemente necessários.

Uma estrutura para avaliar o impacto na futura competição e conflito militar

Informações e inteligência – e o grau de acesso e controle dos sistemas nos quais os dados residem – podem gerar poder e influência em escala. Esses sistemas e as redes que eles criam coletivamente compõem o que caracterizamos como Infraestrutura Digital. Proveniente do crescimento da internet e da interconectividade das redes globais de telecomunicações, a infraestrutura digital de hoje – e a propriedade, o acesso e o controle de um país sobre ela – emergiu como uma área de competição entre os Estados Unidos e a China. Pequim e Washington contam com a infraestrutura digital para apoiar as forças militares e usar as suas capacidades para expandir o poder nacional e estender a influência globalmente. Ambos os países agora pretendem moldar a infraestrutura digital de forma que se alinhe com as suas prioridades e interesses estratégicos de longo prazo.

A nossa hipótese é que, assim como os Estados Unidos veem a presença militar no exterior como um meio estratégico para competir e dissuadir, a República Popular da China também vê a infraestrutura digital como um meio estratégico para a competição. Enquanto a infraestrutura digital afeta várias dimensões do poder, os Estados Unidos e a China abordam-no de maneira diferente.

Para encontrar um porto seguro numa tempestade cibernética

A infraestrutura crítica raramente é manchete – não até que algo dê muito errado – e o sistema de transporte marítimo (MTS) não é exceção. O MTS, responsável pelo transporte seguro da maior parte do comércio internacional, é vital para a economia global. Da carga acumulada em instalações portuárias durante a pandemia de Covid-19 ao navio porta-contentores *Ever Given* bloqueando o Canal de Suez, eventos recentes destacaram a vulnerabilidade do transporte marítimo e o impacto que as interrupções nesse sistema podem ter na vida cotidiana.

De um modo geral, o MTS consiste em todas as vias navegáveis, veículos e portos que são usados para mover pessoas e mercadorias por meio da água. O volume de mercadorias movimentadas dessa forma é particularmente impressionante, com a maior parte da carga mundial sendo transportada por mar – entre 70% e 90%, dependendo de como a carga é contabilizada. Para os Estados Unidos, o MTS contribui com quase 25% do produto interno bruto, totalizando cerca de US$ 5,4 triliões. Também é essencial para a capacidade dos EUA de projetar poder militar. Hoje, como no século passado, o transporte marítimo – o uso de navios de carga para desdobrar recursos militares – é responsável pelo transporte da grande maioria do material militar dos EUA em todo o mundo.

SUGESTÕES DE LEITURA

O ataque da Rússia à Ucrânia provocou ondas de choque na Europa e no mundo. Embora a guerra atual seja um ponto de viragem geopolítico, ainda não está claro se ela desencadeará um salto quântico para as políticas de defesa europeias e para o papel da União Europeia como provedora de segurança. A segurança europeia deu alguns passos importantes desde que se tornou parte das atribuições da UE em 1992. No entanto, três décadas após a sua primeira incursão, continua sendo um projeto incompleto. Em nenhum lugar isso foi mais fácil de ver do que na resposta da UE à crise na Ucrânia. Tal como aconteceu com muitas outras crises do passado recente, a invasão da Ucrânia pela Rússia suscitou uma resposta comum dos Estados-Membros da UE. De facto, ainda mais do que em outras crises, os países encontraram um terreno comum muito rapidamente, em apenas alguns dias e semanas após o 24 de fevereiro. Os países da zona do euro levaram meses, e muitas vezes até anos, para chegar a um acordo sobre uma série de ferramentas comuns para reduzir o risco de repetir outra crise da dívida e melhorar a sua resiliência diante de uma nova (2011-2014).

Em 21 de março de 2022, os ministros da defesa e das relações exteriores da União Europeia adotaram a Bússola Estratégica, com os Chefes de Estado e de Governo da UE subsequentemente endossando-a em 24 de março de 2022. A Bússola Estratégica é uma estrutura acionável para a segurança e defesa da UE até 2030. Ela define ações e cronogramas concretos, com 51 das 81 entregas listadas no documento a serem implementadas até o final de 2022. Antes da reunião do Conselho Europeu de 15 de dezembro de 2022, onde a implementação da Bússola Estratégica será um ponto central tópico de discussão – com base num relatório de progresso do Alto Representante – esta análise aprofundada examina o estado de implementação dos produtos tangíveis na Bússola Estratégica, bem como as oportunidades e desafios que temos pela frente. Após uma introdução sobre os desenvolvimentos recentes na área da defesa da UE, a análise passa a olhar para o 'ato'; 'seguro'; capítulos investir' e 'parceiros' da Bússola Estratégica individualmente.

Com o mundo no meio da primeira crise global de energia – desencadeada pela invasão russa da Ucrânia – o *World Energy Outlook 2022* (WEO) fornece análises e perspetivas indispensáveis sobre as implicações desse choque profundo e contínuo nos sistemas de energia em todo o mundo. Com base nos dados mais recentes sobre energia e desenvolvimentos do mercado, o WEO deste ano explora as principais questões sobre a crise: será um revés para as transições de energia limpa ou um catalisador para uma ação maior? Como as respostas do governo podem moldar os mercados de energia? Quais riscos de segurança energética estão à frente no caminho para emissões líquidas zero? O WEO é a fonte de análise e projeções mais confiável do mundo da energia.
Os seus dados objetivos e análises imparciais fornecem perceções críticas sobre o suprimento e demanda global de energia em diferentes cenários e as implicações para a segurança energética, metas climáticas e desenvolvimento económico.

Com um renovado sentido de urgência associado à rápida evolução da situação geopolítica, o relatório de prospetiva estratégica de 2022, «Geminação das transições ecológica e digital no novo contexto geopolítico», apresenta uma perspetiva abrangente e virada para o futuro sobre a interação entre as duas transições até 2050.
As transições são prioridades da agenda política da União Europeia e a sua interação terá enormes consequências para o futuro. Embora de natureza diferente e sujeitas a dinâmicas específicas, a sua geminação, isto é, a capacidade para se reforçarem mutuamente, merece uma análise mais rigorosa. Compreender melhor estas interações é fundamental para maximizar as sinergias e minimizar os pontos de tensão e é essencial no atual contexto geopolítico, em que a UE visa acelerar as transformações ecológica e digital, reforçando, em última análise, a resiliência e a autonomia estratégica aberta da União Europeia.

O mundo agora enfrenta uma ampla gama de potenciais guerras e crises. O que é muito menos óbvio é o nível total de confronto que se desenvolveu entre os EUA e os seus parceiros estratégicos e a Rússia, o nível semelhante de confronto com a China e o aumento de outros tipos de violência e conflito potencial que estão surgindo num nível global.
A avaliação mostra que a guerra não precisa significar conflito militar real entre as nações envolvidas. Evitar ou minimizar o combate real nunca significou paz. Como Sun Tzu apontou na Arte da Guerra há mais de 2.000 anos, a "guerra" não precisa envolver o uso de força militar ou qualquer forma de combate real. A sua declaração de que "a arte suprema da guerra é subjugar o inimigo sem lutar" refletia muitos dos conflitos na China da sua época. Aplicou-se a outros Estados e culturas ao longo da história e aplica-se a muitos dos confrontos e conflitos de áreas cinzentas que existem hoje.

Uma reflexão crítica

O entrelaçamento entre a inovação, a expansão das tecnologias digitais e a insegurança tem contribuído para o surgimento de preocupações relacionadas com o desenvolvimento de capacidades e capacidades cibernéticas, ou seja, ter meios para responder à insegurança cibernética através da mobilização de recursos tecnológicos, humanos, estratégicos e recursos económicos. Embora alguns estudiosos tenham-se envolvido criticamente com o conceito de "capacidades cibernéticas", a maior parte da literatura permanece associada à consolidação de uma agenda positiva sobre o tema. Com base na literatura de Relações Internacionais, economia política internacional e estudos de desenvolvimento, é oferecida uma análise da formação de uma agenda internacional de desenvolvimento para segurança cibernética, olhando especificamente para as consequências da articulação do conceito de capacidades cibernéticas (o que é necessário, aceitável, desejável e inovador na resposta às ameaças cibernéticas) como um fator-chave para definir visões específicas sobre o que é 'ser capaz' e 'desenvolvido'. Isso também contribui para uma avaliação crítica das desigualdades e assimetrias de poder embutidas em tais projetos de desenvolvimento, com foco particular nos países do Sul Global.

Fazendo um balanço da abordagem da União Europeia

As tecnologias digitais complicam e transformam cada vez mais os conflitos atuais. A atual guerra entre a Rússia e a Ucrânia, por exemplo, também se desenrola no ciberespaço, envolvendo múltiplos atores públicos e privados. Isso varia desde a formação de um exército de TI de voluntários ucranianos até a intensificação de operações cibernéticas maliciosas apoiadas pelo Kremlin, até nações aliadas ocidentais oferecendo assistência à Ucrânia.