idn brief

julho de 2022

SEGURANÇA E DEFESA DO CIBERESPAÇO

CIBERDEFESA, CIBERDISSUASÃO E PODER NACIONAL NO CIBERESPAÇO
Alexandre Lino Marques Pinho

O OBSERVATÓRIO DE CIBERSEGURANÇA
António Gameiro Marques

A TÃO DESEJADA MASSIFICAÇÃO DA CIBER-RESILIÊNCIA ESTÁ A CHEGAR
Francisco Nina Rente

AMEAÇAS HÍBRIDAS: O CIBERESPAÇO NA GUERRA RÚSSIA-UCRÂNIA
Hélder Fialho de Jesus

SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA: A INDISPENSABILIDADE DA GOVERNAÇÃO
João Manuel Assis Barbas

DIRETORA
Isabel Ferreira Nunes
COORDENADOR EDITORIAL
Luís Cunha
CENTRO EDITORIAL
António Baranita e Luísa Nunes
PROPRIEDADE, DESIGN GRÁFICO E EDIÇÃO
Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa
Tel +351 211 544 700
idn.publicacoes@defesa.pt
ISSN 2182-5327
Depósito Legal 340906/12

idn Instituto da Defesa Nacional

Segurança e Defesa do Ciberespaço

Ciberdefesa, Ciberdissuasão e Poder Nacional no Ciberespaço

Alexandre Lino Marques Pinho
Auditor de Defesa Nacional; BA (Hons)
University of Kent.

Muitos vaticinaram que o cenário de guerra entre a Ucrânia e a Federação Russa reunia os elementos necessários para se afirmar como um conflito verdadeiramente cibernético. Esta expectativa assentava na premissa de que a Federação Russa, com reconhecida superioridade no ciberespaço, iria concentrar uma parte substancial do seu esforço no emprego de ações que visassem a disrupção da infraestrutura digital da Ucrânia, potenciando a rápida concretização da "operação militar especial". Recentemente, porém, tem-se referido que essa dimensão do conflito se teria revelado incipiente, tendo alguns editoriais – *The Washington Post* e *The Economist* – afirmado que o apocalipse dos ciberataques que se aguardava afinal não teria acontecido, circunstâncias que têm gerado perplexidade. Importa confrontar estas análises e abordar as potenciais lições a retirar deste conflito.

«Não têm existido ciberataques significativos» – Em relação às operações cibernéticas que se suspeita terem origem russa – provenientes dos serviços GRU, SVR e FSB, e afiliados –, a Microsoft anunciou ter registado 237 incidentes contra a Ucrânia entre dezembro de 2021 e março de 2022, incluindo 40 ciberataques que provocaram a destruição digital de informação em centenas de sistemas através do uso de *software* malicioso.[1] A maior parte destes ciberataques foram direcionados contra setores e infraestruturas críticas – governo, energia, comunicações, controlo de fronteiras e alvos civis –, informação que também foi reportada pelo Cyber Peace Institute. Dias antes de 24 de fevereiro foi atacada a rede de satélites *KA-SAT* operada pela Viasat o que comprometeu a disponibilidade e o funcionamento dos sistemas de comunicações usados pelas autoridades e empresas ucranianas e afetou clientes de outras geografias. Este incidente foi condenado pela União Europeia (UE) e Estados-membros através de uma posição divulgada pelo Alto Representante da União, tendo sido atribuída à Rússia a autoria do ciberataque. Os efeitos provocados pelos ciberataques estão, na sua maioria, em consonância com os eixos de progressão das forças convencionais russas, evidenciando alguma complementaridade entre ações cinéticas e não-cinéticas na conquista de objetivos militares específicos. Refira-se que a Rússia e a Ucrânia têm-se apoiado em entidades externas ou *proxies* para provocar efeitos e disrupções nos sistemas/redes do adversário.[2] De resto, outros ataques – DDoS, *defacements*, etc. – perturbaram o ambiente de informação da Ucrânia, incluindo a colocação num site de notícias de

um "*deepfake"* – um vídeo em que Zelensky anunciava a rendição – que foi transmitido na emissão em direto do canal Ukrayina24.

«A capacidade ciber da Rússia é (afinal) limitada» – *O Military Balance* identifica os EUA, a China e a Rússia como as principais potências militares nos domínios cibernético.[3] Os analistas colocam a Rússia no Tier IV – o escalão mais elevado – surgindo destacadamente com capacidade para conduzir operações no e através do ciberespaço, incluindo de natureza ofensiva, que se têm revelado cada vez mais sofisticadas, e de *surveillance* de movimentos subversivos internos.[4] Em 2015 e 2016 diversos ciber-atacantes, alegadamente patrocinados pela Rússia, atacaram empresas energéticas ucranianas e, em 2017, o ataque *ransomware* NotPetya (GRU) constituiu um dos ataques mais devastadores de sempre. Para a doutrina russa, a guerra no domínio da informação é encarada como um paradigma em contínuo que decorre em tempo de paz e que se desenvolve antes e durante o conflito.[5]

«A Ucrânia não tem meios dedicados à ciberdefesa» – Foi a afirmação das autoridades ucranianas, seguindo-se o apelo à mobilização da comunidade de *hackers* para criar uma *IT army*. Isto tem levado alguns especialistas a sugerir que a Ucrânia tem conseguido impedir ciberataques graças a uma capacidade de "ciberdefesa coletiva". Esta situação não pode deixar de nos surpreender atendendo ao elevado número de ataques que foram perpetrados contra a Ucrânia desde 2014 e que desencadearam a cooperação com países e empresas ocidentais na área da cibersegurança.

Lições do conflito em curso? A afirmação do ciberespaço como 5.º domínio operacional e a presença da componente ciber na preparação e condução dos conflitos, incluindo os efeitos colaterais nos sistemas de Países que não são os alvos diretos dos ciberataques. Indiciou também que o vetor ciber não é suficiente para determinar o resultado de um conflito, quando usado isoladamente. Verificou-se que as informações estratégicas e ISR são fundamentais e que o ambiente de informação permite explorar assimetrias – através de *psyops/infoops* e comunicação estratégica – para compensar algumas fraquezas. E para Portugal? O emprego coordenado destas capacidades e a resposta a ameaças híbridas requer articulação entre estruturas, unidade de direção e verdadeira unidade de esforço; surge reforçada a necessidade de nos dotarmos de uma capacidade de ciberdefesa flexível capaz de ser orientada para a vertente defensiva e a vertente ofensiva, designadamente a exploração proactiva do ciberespaço do oponente. Estas funções são indispensáveis para uma ciber-dissuasão credível e efetiva. Para um país como Portugal a ciber-dissuasão só é robusta se for construída e apoiada na dissuasão por negação que permita impedir ou diminuir os efeitos de ações hostis contra o interesse nacional [6]; Portugal dispõe de garantias no quadro da NATO e da UE, porém, numa resposta ofensiva da NATO, a integração dos *Sovereign Cyber Effects Provided Voluntarily by Allies* constitui, como é explícito, uma decisão soberana e voluntária dos aliados com essas capacidades.[7] Assim, deve privilegiar-se a cooperação bilateral com aliados que possuam capacidades superiores e maturidade doutrinária, com princípios idênticos de soberania digital e com os quais Portugal tem posições concertadas/comuns no âmbito da ciberdefesa, podendo contribuir para uma estratégia de contrapeso e de partilha de informação perante um cenário de ausência de consensualização política na resposta a incidentes de ciberdefesa. Outra componente desta dissuasão por negação alargada passa por enquadrar o envolvimento estruturado de outros intervenientes da sociedade, que podem ter um papel supletivo na eventualidade de enfrentarmos uma situação de crise prolongada, contribuindo assim para a resiliência digital nacional.

[1] Microsoft (2022). An overview of Russia's cyberattack activity in Ukraine.

[2] Reuters (08-03-2022). Russian, Belarusian hackers target Ukraine in phishing.

[3] IISS (2022). Military Balance.

[4] Belfer Center (2020). National Cyber Power Index.

[5] Russian Federation (2016). National Information Security Doctrine e (2021) National Security Strategy.

[6] HCSS (2022). Promises & Perils of Cyberdeterrence.

[7] Paulo Viegas Nunes (2020). A Edificação da Capacidade de Ciberdefesa Nacional. IUM

O Observatório de Cibersegurança

António Gameiro Marques

Contra-Almirante
Autoridade Nacional de Segurança
Diretor-Geral do Gabinete Nacional de Segurança

Todos sabemos que não basta desenvolver estratégias para atingir objetivos em face de um determinado contexto. É também necessário criar um plano de ação que consubstancie essa estratégia, incluindo um modelo de governação da respetiva execução, de modo a adequar dinamicamente as linhas de ação e os recursos disponíveis para atingir os objetivos que foram estabelecidos.
Todavia, muitas vezes os efeitos da consecução das iniciativas que corporizam essa estratégia não são os inicialmente esperados, o que leva a que se deva adequar com rapidez o plano de ação inicialmente gizado.
Esta foi uma das motivações que levou a que, há cerca de quatro anos, o Observatório de Cibersegurança[1] fosse criado, através do qual se procura observar o fenómeno da cibersegurança em Portugal nas suas mais variadas componentes, de modo a informar as partes interessadas e a suportar a definição de políticas públicas de forma cíclica, aplicando-se desta forma o ciclo PDCA (Plan-Do-Check-Act) ao processo. Com uma visão multidisciplinar da sociedade no âmbito do tema da cibersegurança, o Observatório sistematiza e promove a recolha de informação disponível nos domínios da sociedade, economia, políticas públicas, ética e direito, riscos e conflitos, bem como inovação e tecnologias futuras.
Na linha de observação "Sociedade", pretende-se avaliar as atitudes e os comportamentos dos seres humanos na sua relação com a tecnologia e com a segurança inerente. Compreende os valores, as perceções e as ações de utilizadores, técnicos e decisores neste domínio, no que se incluem também a capacitação da sociedade, nas componentes educação e sensibilização. Já existem 3 edições deste relatório (2019, 2022 e 2021), sendo já possível percecionar a evolução da nossa sociedade a este respeito.
A linha de observação "Economia" visa aferir os custos, os investimentos e o mercado existente na sociedade no que diz respeito à prevenção das ciberameaças ou a reação a ciberataques. Foi recentemente publicado o primeiro relatório alusivo a esta linha de observação, o qual contém informação de assinalável relevo, quer relativamente à forma como as empresas portuguesas incorporam a cibersegurança nos seus investimentos, quer quanto à dimensão do mercado de cibersegurança no nosso País.
Um dos objetivos do Observatório é dotar os decisores públicos com a informação pertinente para a criação de políticas públicas informadas e pertinentes em face da situação do País nesta matéria, efetuando simultaneamente um mapeamento das políticas que são desenvolvidas de modo a viabilizar a compreensão da posição relativa de Portugal com outros países neste domínio.
A linha de observação "Políticas Públicas" pretende responder a este requisito. Neste sentido, o 1.º relatório subordinado a este tema já foi publicado, no qual se efetua um levantamento e sistematização tão exaustivo quanto possível, das estratégias e programas públicos relacionados com a cibersegurança, incluindo a identificação e análise de indicadores disponíveis sobre as perceções dos cidadãos quanto aos efeitos decorrentes da implementação dessas mesmas políticas públicas. O documento permite, ainda, conhecer o posicionamento de Portugal no contexto da União Europeia no âmbito desta temática.
De entre os mais diversos desafios, a cibersegurança coloca-nos problemas de natureza legal, fruto da imparável digitalização de muitos processos existentes na nossa sociedade. Paralelamente, surge a ética, enquanto dimensão que reflete sobre o comportamento justo ou correto. A linha de observação "Ética e Direito" recai precisamente sobre os desafios que a segurança do ciberespaço coloca nestes dois domínios, levando em linha de conta a construção de quadros legais e de valores. O primeiro relatório desta linha de observação foi publicado em 2020.
A atualidade tem demonstrado que o ciberespaço é um domínio de eventual confronto entre atores estatais e não estatais, de onde decorrem riscos devido a potenciais conflitos, maioritariamente e cada vez mais de natureza híbrida. Neste contexto, a linha de observação "Riscos e Conflitos" identifica os vários tipos de ameaças e de agentes, de organizações-alvo incluindo os diversos tipos de ataque, procurando caracterizar o modo de relacionamento destas variáveis e os respetivos comportamentos ao longo do tempo. Esta linha de observação é essencial para o desenvolvimento e ajuste de medidas de proteção no ciberespaço. Até à data, foram produzidos três relatórios subordinados a esta linha de observação, relativos a 2020, 2021 e 2022 respetivamente.
A cibersegurança está intrinsecamente ligada ao digital, que é, na atualidade, uma das expressões mais significativas do engenho do ser humano. Importa, por isso, medir

como é que a emergência de novas tecnologias impacta a segurança do ciberespaço. A linha de observação "Inovação e Tecnologias Futuras" procura fazer, quer o levantamento, quer o acompanhamento das práticas científicas em Portugal neste domínio, além de identificar novos desafios à cibersegurança que as aplicações tecnológicas emergentes podem colocar à sociedade no futuro. Está em curso a produção do primeiro relatório sobre esta linha de observação.
Para além das linhas de observação acima mencionadas, foi recentemente publicado um relatório onde se identifica a oferta formativa nacional de cibersegurança ao nível do ensino profissional e superior (universitário e politécnico), de modo a obter-se uma base de partida para o desenvolvimento e projeção da oferta formativa que vai ser consubstanciada através do projeto da C-Academy (Programa nacional de formação avançada em cibersegurança), com a qual se pretende formar 9.600 profissionais até ao fim da primeira metade de 2026.
Em suma, o Observatório de Cibersegurança pretende ser uma plataforma de análise e sistematização de conhecimento, com informação disponível a toda a sociedade, que suscite o debate informado em torno de temas multidisciplinares da cibersegurança, identificando tendências indexadas a referências temporais e articulando as várias partes interessadas na recolha de informação. Este é um contributo do Centro Nacional de Cibersegurança para a criação de conhecimento sustentado em torno do tema na sociedade portuguesa, esperando-se que, paralelamente, proporcione um incremento da respetiva maturidade no domínio da cibersegurança, proporcionado assim decisões mais fundamentadas aos mais diversos níveis no âmbito deste tema.

A Tão Desejada Massificação da Ciber-Resiliência Está a Chegar

Francisco Nina Rente

Co-fundador e CEO da Art Resilia, uma empresa focada em ciber-resiliência. Conta já com mais de 20 anos de experiência nas áreas de ciber-resiliência, cibersegurança e segurança de informação, onde desempenhou funções de gestor, docente, formador, orador, consultor e auditor. Fundou empresas/organizações como a Dognaedis, CodeV e CERT-IPN. Formado em Engenharia Informática pela Universidade de Coimbra.

A informação é cada vez mais o ativo de maior valor de qualquer organização, ditando inclusive a sua performance, estabilidade e resiliência. Mas isto é, finalmente, uma verdade de La Palice. Em contraponto está a consciência da evolução que a cibersegurança tem que ter – a sua transformação em ciber-resiliência.
Nesta nossa era digital, a informação passa quase obrigatoriamente pelo ciberespaço, quer seja na sua produção, trânsito ou armazenamento, ligando desta forma cadeias de valor cada vez mais complexas, dispersas e nem sempre sustentadas por referências geográficas. Por consequência, a ciber-resiliência das organizações tornou-se o principal fator de sua resiliência, tornando o ciberespaço um alvo primário para atividades maliciosas.[1]
Não havendo à data uma definição unânime do que é a ciber-resiliência, comecemos por balizar uma definição: capacidade de antecipar, resistir, recuperar e adaptar-se a estímulos inadvertidos, condições adversas, ataques ou comprometimentos de ativos que usam ou são habilitados por recursos cibernéticos[2]. Por outras palavras, um estado contínuo na evolução da maturidade da cibersegurança, que traz ao tradicional ciclo de identificar, detetar, proteger, responder e recuperar de ciber ameaças, um novo estádio – antecipar e prevenir – bem como um enfoque adicional na recuperação, tornando-a transversal e continuamente disponível. Esta definição é simples de assimilar e enquadra diretamente com o entendimento atual sobre a capacidade a montante, a cibersegurança.
Com base nesta definição ou em eventuais semelhantes, começam a aparecer as primeiras evidências da tão desejada adoção, e por consequência massificação, da ciber-resiliência. Foquemo-nos então no contexto nacional, onde podemos observar:

- A atual Estratégia Nacional de Segurança do Ciberespaço (ENSC), vigente entre 2019 e 2023, estabelece um conjunto de princípios, objetivos estratégicos e seis eixos de ação a implementar em Portugal. Embora não sejam muitas as referências diretas à ciber-resiliência, existe quase de uma forma transversal a referência aos princípios da mesma. Certo é que se apresenta com tendo em "vista a resiliência e a capacidade de resposta rápida e efetiva a ciberataques " no ciberespaço nacional, definindo assim como visão a concretizar até 2023 "que Portugal seja um país seguro e próspero através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade", ou seja, um Portugal mais ciber-resiliente capaz de suportar

uma sociedade democrática saudável, inovadora e próspera.
De entre os objetivos estratégicos definidos na ENSC, logo o primeiro garante a orientação à resiliência. Intitulado como "Maximizar a resiliência", estabelece como objetivos garantir a resiliência digital nacional.

- Recentemente, em Davos-Klosters na Suíça, na reunião anual do Fórum Mundial Económico, um conjunto dos principais atores do sector mundial *Oil and Gas* efetivam uma vontade conjunta de combater os ciberataques ao sector, lutando assim por uma resiliência sectorial. Este acontecimento torna-se especialmente relevante para Portugal visto que um dos principais promotores do mesmo foi a Galp. Andy Brown, enquanto CEO da Galp, frisa publicamente a relevância do acontecido e o empenho da Galp no mesmo – "The pledge advances Galp's commitment to joint action on managing cyber risks and protecting cybersecurity of critical energy infrastructure, by creating awareness and a unified stance on cyber resilience in the global energy sector"[3] .
Pode-se assim concluir que, quer numa realidade pública quer privada, Portugal começa a ter posicionamentos e estratégias bem definidas e claramente orientadas à ciber-resiliência.
Estando já em andamento esta transformação, torna-se premente perceber concretamente o que são as adições que a ciber-resiliência traz à defesa contra ciber-ameaças. Como já referido, a montante surge a antecipação, uma capacidade focada em ameaças futuras (ou não efetivadas) que se constrói sobre uma monitorização específica de atores de ameaça e abordagens de defesa pré-ataque e auto-evolutivas.
Esta monitorização específica, de que a antecipação carece, apresenta-se como obrigatoriamente proactiva e exploratória, que compreenda ambas as esferas interna e externa (à organização). Tecnicamente, assenta em diversos mecanismos de armadilha – na camada de rede e aplicacional – e nos mais típicos procedimentos de rastreio e recolha de dados não estruturados, dando-lhe à posterior estrutura e significado, ou seja, transformando-os em inteligência.
Já as abordagens de defesa típicas da antecipação, caracterizadas como de pré-ataque – bloqueio às fases pré-ataque tais como a capacitação, implementação de infraestrutura de suporte ao ataque ou reconhecimento de alvos – e auto-evolutivas – moldam as suas capacidades de reação mediante as ações do agente de ameaça –, são provavelmente a componente da ciber-resiliência mais complexa de implementar tecnicamente. Algo que, embora não existam soluções completas, é perfeitamente passível de ser implementado, quer com recurso a soluções proprietárias quer com soluções baseadas em *open source*.
Por último, relativamente ao enfoque adicional que a ciber-resiliência exige em relação à capacidade de recuperação, é importante dizer que a sua efetividade embora esculpida por políticas e processos, apenas é verdadeiramente materializável de forma a ser útil se consistir numa abordagem transversal a toda a organização e continuamente disponível.

[1] Disponível em https://www.weforum.org/projects/cyber-resilience-index

[2] Disponível em https://csrc.nist.gov/glossary/term/cyber_resiliency

[3] Disponível em https://www.weforum.org/press/2022/05/global-ceos-commit-to-collective-action-on-cyber-resilience-ffa0ba5f56

Ameaças Híbridas: O Ciberespaço na Guerra Rússia-Ucrânia

Hélder Fialho de Jesus

Capitão-de-mar-e-guerra.

A presente realidade de conflito entre a Rússia e a Ucrânia, com a destruição e a perda de vidas, constitui-se como um *continuum* de situações que tem o seu histórico, mas que agora se agravou. Num antagonismo latente entre estes dois países, o ciberespaço tem sido utilizado como um elemento de afirmação e de confrontação, sendo os ataques a infraestruturas críticas, na área da energia, um dos muitos exemplos. Recuando a dezembro de 2015, relembra-se que a cidade de Kiev e a parte ocidental do país ficaram sem energia por várias horas, afetando mais de 200 000 pessoas, inibições idênticas que se repetiram em anos seguintes.
Não havendo uma definição consensual sobre ameaças híbridas ou guerra híbrida, podemos ter como referência o "The Landscape of Hybrid Threats: A Conceptual Model", publicado em 2021 pelo European Centre of Excellence for Countering Hybrid Threats (HybridCoe).
Aqui é referido que, para além do contexto científico e militar, os termos "ameaças híbridas" e "guerra híbrida" também são aplicados no contexto político, situação esta que decorreu da anexação da Crimeia em 2014. Estabelece ainda que o uso político de Ameaças Híbridas se refere à interferência manipuladora e

indesejada por meio de uma variedade de ferramentas: disseminação de desinformação e *fake news*, criação de narrativas históricas fortes – incorretas ou apenas parcialmente corretas –, interferência eleitoral, ataques no ciberespaço, influência económica, entre outros.

Tendo em conta que o ciberespaço se constitui como um domínio das operações militares, pretende-se neste artigo mostrar algumas das situações ocorridas neste espaço, no contexto da atual guerra no leste europeu, tendo por base fontes abertas.

Neste sentido, importa assinalar o recente relatório da Microsoft, intitulado "The hybrid war in Ukraine" publicado em finais de abril, que retrata bem a relação entre o ciberespaço e as operações militares físicas no mundo real, muitas delas cinéticas. De notar que as observações apresentadas revelaram que grupos ligados aos serviços de informações russos começaram a preparar o terreno para incursão militar ainda em 2021. Neste contexto, foi referido que grupos de *hackers* acederam a redes serviços críticos, particularmente nas áreas das Tecnologias de Informação e Comunicação (TIC) e da energia ucranianos. A realidade veio mostrar que alguns desses alvos foram atingidos posteriormente em 2022, com vírus destrutivos que eliminaram dados (Viper) e desativaram computadores.

Mas a partir de janeiro de 2022 foram várias as evidências da utilização do ciberespaço no contexto da presente guerra e que foram sentidas na sociedade Ucraniana e não só. Assim, a 14 de janeiro, cerca de 70 *websites* do governo ucraniano e de autoridades regionais viram as suas redes e plataformas web serem atacadas, ficando a maioria sem serviços. Em alternativa, muitas passaram a apresentar uma imagem com mensagens de ameaças em três idiomas (ucraniano, russo e polaco), com o seguinte texto: "Tenha medo e espere o pior".

Neste mesmo período, o Microsoft Threat Intelligence Center (MSTIC) verificou evidências de um *malware* destrutivo, designado de *Whispergate*, em várias organizações na Ucrânia. Este *malware*, apresentava semelhanças ao NotPetya, de 2017, que muitos consideram como sendo o que maior prejuízo causou, tendo Tom Bossert, o ex-assessor de Segurança Interna, referido o valor de 10 mil milhões de dólares.

A data de 24 de fevereiro de 2022, dia da intervenção militar russa, também coincidiu com uma disrupção nos serviços satélite da Viasat, uma empresa de comunicações global com serviço de internet via satélite, afetando milhares de clientes Europa, com especial incidência na Ucrânia. A União Europeia imputou este ataque à Federação Russa, pelo que se pode inferir que esta atividade estaria inserida na operação militar em curso sobre a Ucrânia, preparando o campo de batalha com o corte das comunicações adversárias.

Ainda segundo a Microsoft, numa ligação entre as atividades no ciberespaço e o mundo físico, foi apresentado o ataque cinético com mísseis dirigido à torre de TV de Kiev, ocorrendo no mesmo período em que se verificou um conjunto generalizado de atividades disruptivas no ciberespaço direcionadas para os *media* na capital da Ucrânia. O outro exemplo ocorreu aquando da ocupação da central nuclear de Zaporizhzhia, a maior da Europa, por militares russos, que coincidiu com a infiltração de um grupo russo nas redes de uma empresa de energia nuclear ucraniana.

No entanto, apesar ao acima descrito, as operações no ciberespaço foram em menor número e menos sofisticadas do que muitos esperavam, dada a história anterior nesta zona, particularmente na área as infraestruturas críticas, com relevo para a rede elétrica. De notar que o Departamento de Estado dos EUA, desde 2017, já disponibilizou mais de 40 milhões de dólares à Ucrânia, destinados à resiliência do ciberespaço deste país. Desta forma, podemos afirmar que este apoio terá contribuído significativamente para que os efeitos no ciberespaço neste conflito tenham tido um impacto menor do que o esperado.

Em jeito de conclusão, pode referir-se que atores estatais e não estatais desafiam nações, instituições e empresas por meio de uma ampla gama de atividades, abertas e encobertas, orientadas para as vulnerabilidades adversárias, cuja ação tem implicações na sociedade e na vida das pessoas. Assim, verifica-se que a dimensão híbrida ligada ao ciberespaço tem relevo no presente conflito entre a Rússia e a Ucrânia, mas ainda está longe a sua afirmação, pois a realidade tem demonstrado que a geografia e o mundo físico ainda têm um peso significativo.

Segurança da Informação e Cibersegurança: A indispensabilidade da Governação

João Manuel Assis Barbas
Coronel do Exército. Subdiretor do Curso de Defesa Nacional e Assessor da Diretora do Instituto da Defesa Nacional.

O termo *Corporate Governance* terá sido referido ao tempo da Companhia das Índias associado a responsabilidade de gestão,

estrutura de administração e direitos dos acionistas. Mais recentemente, nos EUA, nos anos 70 do século passado, entrou em voga para expressar e delimitar as relações de poder, com especial enfâse no âmbito financeiro, entre os conselhos de administração, gestão executiva e acionistas. Desde então, o termo *Governance* ou Governação, expandiu-se para outros domínios das organizações. Nesse sentido surgiu a noção de *Governance of IT* abordada em diversas normas da ISO (International Standards Organization) e ISACA[1] (COBIT5[2]), visando apoiar as organizações nos domínios da conformidade (*compliance*), gestão de riscos e alinhamento estratégico das Tecnologias de Informação com os objetivos organizacionais.

Com as crescentes preocupações com a Segurança da Informação e a Cibersegurança, a ISO publicou uma norma dedicada à Governação da Segurança da Informação[3], posteriormente expandida para a Cibersegurança e Privacidade[4], com orientações para a avaliação, orientação, monitorização e comunicação das atividades das organizações nesses domínios. Ela realça a importância do alinhamento estratégico com os objetivos organizacionais, a exigência de conformidade legal, regulamentar e contratual, a gestão do risco e o controlo interno, e a criação de valor para todas as partes interessadas. É ainda identificada a necessidade de desenvolver um modelo de governação corporativa que permita compatibilizar as diversas áreas de governação existentes nas organizações – ex. Finanças, Recursos Humanos, Tecnologias de Informação, etc.

Entretanto e desde 2012, o World Economic Forum (WEF) chamou à atenção para a noção de Ciber-resiliência (*Cyber Resilience*) atendendo à inevitabilidade dos ciberataques nas sociedades com elevadas taxas de penetração de infraestruturas e serviços digitais e à exigência de capacidade de reação das organizações face a essas adversidades. O WEF enfatizou a indispensabilidade da governação, através da liderança (da gestão de topo), responsabilização e conformidade nas questões da Cibersegurança, e integração da gestão do risco da segurança da informação na gestão do risco corporativo, tendo proposto um conjunto de princípios orientadores[5]. A CPMI-IOSCO[6] propôs também um conjunto de orientações para a ciber-resiliência das infraestruturas do mercado financeiro (FMI), considerada indispensável para a sua estabilidade. Esse documento realçou a importância da governação, através de um quadro de referência compreensivo para a ciber-resiliência, com uma estratégia específica alinhada com os objetivos e requisitos de eficiência da operação das FMI, em consonância com outras formas de risco, e atendendo aos requisitos da gestão do risco.

Em síntese, a governação é indispensável à Segurança da Informação e Cibersegurança, podendo ser definida como o "sistema pelo qual as atividades de segurança da informação de uma organização são dirigidas e controladas"[7]. A enfâse colocada na governação da Segurança da Informação e da Cibersegurança pelas normas e publicações referidas suscita algumas interrogações quanto às práticas das organizações. Nesse sentido, (Volchkov, 2018) evidencia situações que caracterizam limitações nesse domínio:

- A concentração da responsabilidade pela implementação de controlos de segurança exclusivamente numa única estrutura orgânica, normalmente pelas TI;

- O não envolvimento da administração / gestão de topo da organização nas decisões estratégicas da Segurança da Informação / Cibersegurança por se considerar não qualificada para o efeito;

- A indisponibilidade de recursos para implementar as políticas de segurança da organização superiormente aprovadas;

- A inexistência de prévia avaliação de segurança de projetos ou identificação de riscos, de acordo com as políticas de segurança;

- A falta de relatórios de situação e/ ou monitorização da adequação e eficácia dos controlos/mecanismos de segurança implementados.

A norma ISO/IEC 27002:2022[8] contempla quatro tipo de controlos de segurança: organizacionais, humanos, físicos e tecnológicos. Como tal, a sua implementação deverá em princípio ser realizada pelas estruturas internas de acordo com as respetivas responsabilidades funcionais, a estratégia e política de segurança da organização e em articulação com a respetiva organização de segurança. De acordo com os princípios da norma ISO/IEC 27014, a administração / gestão de topo de uma organização é responsável, nomeadamente, por:

- Dirigir os processos de governação da organização, nomeadamente, a sua estratégia e objetivos, alocação de recursos, priorização de atividades, aprovação de políticas e tomada de decisão sobre gestão de risco;

- Monitorizar a concretização dos objetivos estratégicos, nomeadamente, a eficácia da gestão das atividades da segurança da informação, a conformidade com os requisitos legais

e normativos internos e externos, e o seu potencial impacto em caso de alteração.
A (boa) governação não elimina outros requisitos do desenvolvimento da capacidade de Segurança da Informação e ou Cibersegurança de uma qualquer organização, mas é um elemento fundamental que importa concretizar em prol de organizações mais ciber-resilientes.

[1] Information Systems Audit and Control Association.

[2] Control Objectives for Information and Related Technology.

[3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION [ISO] 2013. ISO/IEC 27014: 2013 Information technology—Security techniques—Governance of information security.

[4] INTERNATIONAL STANDARDS ORGANIZATION (ISO) 2020. ISO/IEC 27014:2020 (en) Information security, cybersecurity and privacy protection — Governance of information security.

[5] World Economic Forum, 2017. Advancing Cyber Resilience: Principles and Tools for Boards. Geneva, Switzerland.

[6] CPMI-IOSCO 2016. Guidance on Cyber Resilience for Financial Market Infrastructures. Committee on Payments and Market Infrastructures–Board of the International Organization of Securities Commissions.

[7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION [ISO] 2013. ISO/IEC 27014: 2013 Information technology—Security techniques—Governance of information security.

[8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION [ISO] 2022. ISO/IEC 27002:2022(en) Information security, cybersecurity and privacy protection — Information security controls.